Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

Grant Agreement No.653426
Topic: DS-01-2014 (Privacy)
Innovation Action

Deliverable D2.1
Legal framework analysis report

Document Number: D2.1
Contractual Date of Delivery: 27.05.16
Editor: UoB
Work-package: WP2
Distribution / Type: Public (PU) /Report (R)
Version: v1.0
Total Number of Pages 103

This deliverable has been written in the context of the Privacy Flag Horizon 2020 European research project, which is supported by the European Commission and the Swiss State Secretariat for Education, Research and Innovation. The opinions expressed and arguments employed do not engage the supporting parties.

Deliverable D2.1 Legal framework analysis report
Abstract:

Privacy Flag (PF) combines crowd sourcing, ICT technology and legal expertise to protect citizen privacy when visiting websites, using smart-phone applications, or living in a smart city. It will enable citizens to monitor and control their privacy with a user friendly solution provided as a smart phone application, a web browser add-on and a public website. It will:

1. Develop a highly scalable privacy monitoring and protection solution with:
   - Crowd sourcing mechanisms to identify, monitor and assess privacy-related risks;
   - Privacy monitoring agents to identify suspicious activities and application;
   - Universal Privacy Risk Area Assessment Tool and methodology tailored on European norms on personal data protection;
   - Personal Data Valuation mechanism;
   - Privacy enablers against traffic monitoring and fingerprinting;
   - User friendly interface informing on the privacy risks when using an application or website.

2. Develop a global knowledge database of identified privacy risks, together with online services to support companies and other stakeholders in becoming privacy-friendly, including:
   - In-depth privacy risk analytical tool and services;
   - Voluntary legally binding mechanism for companies located outside Europe to align with and abide to European standards in terms of personal data protection;
   - Services for companies interested in being privacy friendly;
   - Labelling and certification process.

3. Collaborate with standardization bodies and actively disseminate towards the public and specialized communities, such as ICT lawyers, policy makers and academics. Eleven (-11-) European partners, including SMEs and a large telco operator (OTE), bring their complementary technical, legal, societal and business expertise; Privacy-Flag intends to establish strong links with standardization bodies and international fora and it also intends to assess and incorporate outcomes from over 20 related research projects. It will build and ensure a long term sustainability and growth.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

Executive Summary
This document (D2.1) is linked to the task T2.1 within work package 2 (WP2) of the project. WP2 is focused on Privacy risks analysis and modelling. The document analyses existing legal frameworks with a focus on European and international norms related to personal data protection, privacy and data ownership. It identifies and categorises the:

- personal data protection and privacy obligations and norms that have been developed in key national and supra-national jurisdictions, and which play a primary role in influencing international governmental and commercial practices;
- obligations and norms which have developed and promoted by means of international Guidelines, Agreements and Conventions.

Section 1 offers a brief introductory overview of the work package context.

Section 2 briefly distinguishes between the concepts of privacy, personal data protection and data ownership.

Section 3 discusses international organisations that have contributed towards standards relating to personal data protection and privacy, focusing on the United Nations, Organisation for Economic Co-operation and Development, Council of Europe, World Trade Organisation and International Telecommunications Union.

Section 4 discusses the European framework relating to personal data protection and privacy, focusing on the EU Directives and General Data Protection Directive, as well as the role of the European Convention on Human Rights.

Section 5 discusses a range of international regional frameworks and national regimes relating to personal data protection and privacy, focusing upon the US and Canada as common law jurisdictions, Latin America, the APEC and ECOWAS regional frameworks, and 3 examples of non-EU national jurisdictions at various stages of developing data privacy regimes, China, India and Russia.

Section 6 provides a set of clear and concise legal requirements via a synthesis of the legal risks that the Privacy Flag project will address.

Finally, section 7 offers a summary of the key issues discussed in the document.
## Contributors

<table>
<thead>
<tr>
<th>First name</th>
<th>Last name</th>
<th>Partner</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew</td>
<td>Charlesworth</td>
<td>UOB</td>
<td><a href="mailto:a.j.charlesworth@bristol.ac.uk">a.j.charlesworth@bristol.ac.uk</a></td>
</tr>
<tr>
<td>Ioannis</td>
<td>Chochliouros</td>
<td>OTE</td>
<td><a href="mailto:ichochliouros@oteresearch.gr">ichochliouros@oteresearch.gr</a></td>
</tr>
<tr>
<td>Camilla</td>
<td>Bistolfi</td>
<td>IIP</td>
<td><a href="mailto:bistolfi@istitutoitalianoprivacy.it">bistolfi@istitutoitalianoprivacy.it</a></td>
</tr>
<tr>
<td>George</td>
<td>Yannopoulos</td>
<td>UoA</td>
<td><a href="mailto:gyannop@law.uoa.gr">gyannop@law.uoa.gr</a></td>
</tr>
<tr>
<td>Alexandros</td>
<td>Tsakrilis</td>
<td>UoA</td>
<td><a href="mailto:alextsak@di.uoa.gr">alextsak@di.uoa.gr</a></td>
</tr>
<tr>
<td>Panagiotis</td>
<td>Kontopoulos</td>
<td>UoA</td>
<td><a href="mailto:pkontopoulos@di.uoa.gr">pkontopoulos@di.uoa.gr</a></td>
</tr>
<tr>
<td>Nikos</td>
<td>Bompetsis</td>
<td>UoA</td>
<td><a href="mailto:nbompetsis@di.uoa.gr">nbompetsis@di.uoa.gr</a></td>
</tr>
<tr>
<td>Nancy</td>
<td>Alonistioti</td>
<td>UoA</td>
<td><a href="mailto:nancy@di.uoa.gr">nancy@di.uoa.gr</a></td>
</tr>
<tr>
<td>Sébastien</td>
<td>Ziegler</td>
<td>MI</td>
<td><a href="mailto:sziegler@mandint.org">sziegler@mandint.org</a></td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM</td>
<td>Association for Computing Machinery</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation Forum</td>
</tr>
<tr>
<td>CAHDATA</td>
<td>Ad hoc Committee on data protection</td>
</tr>
<tr>
<td>CBPR</td>
<td>Cross Border Privacy Rules System (APEC)</td>
</tr>
<tr>
<td>CCPR</td>
<td>Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>CFREU</td>
<td>Charter of Fundamental Rights of the EU</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CPEA</td>
<td>Cross-Border Privacy Enforcement Arrangement (APEC)</td>
</tr>
<tr>
<td>CRC</td>
<td>Convention on the Rights of the Child</td>
</tr>
<tr>
<td>CRTA</td>
<td>Cross-regional trade agreement</td>
</tr>
<tr>
<td>CTU</td>
<td>Caribbean Telecommunications Union</td>
</tr>
<tr>
<td>DP</td>
<td>Data Protection</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authorities</td>
</tr>
<tr>
<td>DPD</td>
<td>Data Protection Directive (EU)</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>DS</td>
<td>Digital Security</td>
</tr>
<tr>
<td>EAC</td>
<td>East African Community</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECourtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>ECOWAS</td>
<td>Economic Community of West African States</td>
</tr>
<tr>
<td>ETS</td>
<td>European Treaty Series</td>
</tr>
<tr>
<td>EU</td>
<td>European Union European Convention on Human Rights</td>
</tr>
<tr>
<td>FIPs</td>
<td>Fair Information Practices</td>
</tr>
<tr>
<td>FTA</td>
<td>Free Trade Agreement</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>GA</td>
<td>General Assembly</td>
</tr>
<tr>
<td>GA</td>
<td>Grant Agreement</td>
</tr>
<tr>
<td>GATS</td>
<td>General Agreement on Trade in Services (WTO)</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation (EU)</td>
</tr>
<tr>
<td>H2020</td>
<td>Horizon 2020</td>
</tr>
<tr>
<td>HRC</td>
<td>Human Rights Council</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT-A</td>
<td>IoT Architecture</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>KORUS</td>
<td>Korea-US Free Trade Agreement</td>
</tr>
<tr>
<td>MIIT</td>
<td>Ministry of Industry and Information Technology (China)</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>OJ</td>
<td>Official Journal</td>
</tr>
<tr>
<td>PEA</td>
<td>Privacy Enforcement Authority (APEC)</td>
</tr>
<tr>
<td>PDPO</td>
<td>Personal Data Protection Officer</td>
</tr>
<tr>
<td>PF</td>
<td>Privacy Flag</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
<tr>
<td>PII</td>
<td>Personally identifying information</td>
</tr>
<tr>
<td>RIPD</td>
<td>Ibero-American Data Protection Network</td>
</tr>
<tr>
<td>SACAPDS</td>
<td>Secretary’s Advisory Committee on Automated Personal Data Systems</td>
</tr>
<tr>
<td>SADC</td>
<td>Southern African Development Community</td>
</tr>
<tr>
<td>SME</td>
<td>Small- and Medium-sized Enterprise</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SC-NPC</td>
<td>Standing Committee of the National People’s Congress (China)</td>
</tr>
<tr>
<td>TiSA</td>
<td>Trade in Services Agreement (EU/US)</td>
</tr>
<tr>
<td>T-PD</td>
<td>Consultative Committee on Convention 108 (CoE)</td>
</tr>
<tr>
<td>TTIP</td>
<td>Transatlantic Trade and Investment Partnership (EU/US)</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNCTAD</td>
<td>United Nations Conference on Trade and Development</td>
</tr>
<tr>
<td>UNHRC</td>
<td>United Nations High Commissioner for Refugees</td>
</tr>
<tr>
<td>UNHRC</td>
<td>UN Human Rights Council</td>
</tr>
<tr>
<td>UPRAAM</td>
<td>Universal Privacy Risk Area Assessment Methodology</td>
</tr>
<tr>
<td>UPRAAT</td>
<td>Universal Privacy Risk Area Assessment Tool</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>WP</td>
<td>Working Party</td>
</tr>
<tr>
<td>WPL</td>
<td>Work Package Leader</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
Definitions
Those definitions are derived from those listed in the prior PF Deliverable D1.1, in order to ensure the coherence of the whole work in terms of the interpretation of privacy and data protection concepts. However, they have been revised in light of the final approved version of the General Data Protection Regulation (GDPR) ¹ and all the references to its Recitals and Articles have been provided.

A –
Adequacy decision. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection² with the so-called “adequacy decision” (see definition of “Data transfer” below). In the absence of such a decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These “appropriate safeguards” may consist of: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules (see definition below); standard data protection clauses adopted by the Commission or by the supervisory authority and approved by the Commission; an approved code of conduct or certification mechanism both adopted with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ right.³

Accountability. Principle that guarantees data controller’s compliance with data protection principles, through the adoption of technical and internal measures.

Anonymization. A technique applied to personal data in order to achieve irreversible de-identification.⁴


B –
Binding corporate rules. Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers, or a set of transfers, of

---
² Art.45(1), GDPR.
³ Art.46(2), GDPR
personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.\footnote{Art.4(20), GDPR.}

Biometric data. Any data relating to the physical, physiological or behavioural characteristics of an individual, which allow their unique identification, such as facial images, or dactyloscopic data (fingerprints).\footnote{Art.4(14), GDPR.}

Biometric systems. Methods for uniquely recognizing humans with a high level of accuracy, though one or more physical or behavioural traits.

\textbf{C – Certifications.} Data protection certification mechanisms are seals or marks established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are subject to the GDPR. Within the framework of personal data transfers to third countries or international organisations, the certification can be used as “adequate safeguard” in lack of an adequacy decision of the Commission for the data transfer (see definition of “Adequacy decision” above), so it can be used also by the controller or processor not established in EU. The controller or processor of third countries will also make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.\footnote{Art.42, GDPR.}

Codes of conduct. A code of conduct is an approved mean for specifying the application of the GDPR itself – e.g. identifying the conditions of fair and transparent processing; the legitimate interests pursued by controllers in specific contexts; the conditions of the collection of personal data; the use of pseudonymisation; the information provided to the public and to data subjects; the way to exercise the rights of data subjects; the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; the implementation of privacy by design and by default principles etc. The drawing up of codes of conduct intended to contribute to the proper application of the GDPR. They can be drawn up by associations and other bodies representing categories of controllers or processors (or amend or extend such codes).\footnote{Art.40, GDPR.}

Communication. Any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.\footnote{Art.2(d), Directive 2002/58/EC.}

Confidentiality. It is forbidden to listen, tap, store or realize other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised.\footnote{Art.5(1), Directive 2002/58/EC.}
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

Consent. Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.\textsuperscript{11}

Cookies. Short text files stored by a website on the user’s device to provide more personalised experiences, by remembering user profile without the need of a specific log-in. A “session cookie” is a cookie that is automatically deleted when the user closes his/her browser, while a “persistent cookie” is a cookie that remains stored in the user’s terminal device until it reaches a defined expiration date (which can be minutes, days or several years in the future). A “third party cookie” would thus refer to a cookie set by a data controller that is distinct from the one that operates the website visited by the user (as defined by the current URL displayed in the address bar of the browser).\textsuperscript{12}

Crowdsourcing. The act of taking a job, service, idea or content traditionally performed by a designated agent and outsourcing it to an undefined, generally large group of people in the form of an open call, especially from an online community.

D –

Data breach. Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.\textsuperscript{13} In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.\textsuperscript{14} When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.\textsuperscript{15} Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the competent authority that it has implemented appropriate technological protection measures, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; or that he has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or if the notification to all the individuals concerned would involve disproportionate effort.\textsuperscript{16}

Data concerning health. Any information which relates to the physical or mental health of an individual or to the provision of health services to the individual.\textsuperscript{17}

\begin{itemize}
  \item Art.4(11), GDPR.
  \item Art.29 Data Protection Working Party, \textit{Opinion 04/2012 on Cookie Consent Exemption WP 194, 00879/12/EN (7 June 2012) at 4-5.}
  \item Art.4(12), GDPR.
  \item Art.33(1), GDPR.
  \item Art.34(1), GDPR.
  \item Art.34(3), GDPR.
  \item Art.4(15), GDPR.
\end{itemize}
Data controller. The natural or legal person, public authority, agency or other body which, alone or jointly with others (i.e. joint data controllership, see definition below), determines the purposes and means of the processing of personal data.\(^\text{18}\)

Data processing. Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.\(^\text{19}\)

Data processor. A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.\(^\text{20}\)

Data protection (DP). The set of rights and principles for personal data processing, such as the specific purposes and consent of the person concerned, regardless of whether the data is held in the public or private sector. Article 8 of the Charter of Fundamental Rights of the European Union guarantees data protection as a fundamental right by protecting individuals without impeding the free flow of information, thanks to the legal certainty given to the data subject.\(^\text{21}\)

Data protection officer (DPO). According to the GDPR, where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences, a person should assist the controller or processor to monitor internal compliance with data protection rules.\(^\text{22}\)

Such data protection officers, whether or not an employee of the controller, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices.\(^\text{23}\)

Data recipient. A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of such data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.\(^\text{24}\)

\(^{18}\) Art.4(7), GDPR.

\(^{19}\) Art.4(2), GDPR.

\(^{20}\) Art.4(8), GDPR.

\(^{21}\) “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority”, Art.8, Charter of Fundamental Rights of the European Union, 2012/C 326/02.

\(^{22}\) Art.37(1), GDPR.

\(^{23}\) Art.37(5), GDPR.

\(^{24}\) Art.4(9), GDPR.
Data retention. A processing operation consisting of retaining personal data for certain purposes, including those provided for by law (e.g. investigation, detection and prosecution of serious crimes).

Data subject. An identified or identifiable natural person whose personal data are collected, held or processed. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.\(^\text{25}\)

Data subject’s rights. Part of the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data (see below “Right to be informed”, “Right of access”, “Right to restriction of the processing”, “Right to obtain the notification to third parties”, “Right to object”, “Right not to be subject to a decision” and “Right to be forgotten”).

Data transfer. Any transmission or communication of data to a third country or an international organisation. These transfers shall take place only if all the conditions established by the GDPR (Articles 44-49) are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. See also “Adequacy decision” definition.

E –

European Data Protection Board. According to Recital 139 of the GDPR, the board will replace the Article 29 Working Party established by Directive 95/46/EC (see definition above). It will consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Board will contribute to the consistent application of the GDPR throughout the EU, including advising the Commission on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union, according to Article 70 of the GDPR.

G –

Genetic data. Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.\(^\text{26}\)

Granular consent. Especially when using a smartphone application (app), after asking for consent before data collection, the data controller must ask for granular consent for each type of data the app will access, at least for the categories of: location, contacts, unique device identifier, identity of the data subject, identity of the phone, credit card and payment data, telephony and SMS, browsing history, email, social networks credentials and biometrics.\(^\text{27}\)

I –

Information. Each data subject has the right to know the identity of the data controller who is processing his/her personal data, what type of personal data is being processed and for what

---

\(^{25}\) Art.4(1), GDPR.

\(^{26}\) Art.4(13), GDPR.

purpose the data are intended to be used. Availability of this information on personal data processing is critical in order to obtain consent from the user for the data processing and, for the same reason, this information has to be clear and comprehensive.\textsuperscript{28} (see below “Right to be informed”).

\textbf{J – Joint controllers.} Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information to them. These responsibilities will be determined by means of an arrangement between them unless the respective responsibilities are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.\textsuperscript{29}

\textbf{L – Layered notice.} Where the initial notice to the user contains the minimum information required by the EU legal framework, further information is available through links to the whole privacy policy that has to be readable, understandable and easily accessible.\textsuperscript{30}

\textbf{Location data.} Any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Such data may only be processed when they are anonymised, or with the consent of the users or subscribers, to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.\textsuperscript{31}

\textbf{P – Personal data.} Any information relating to an identified or identifiable natural person (the data subject).\textsuperscript{32}

\textbf{Personal data filing system.} Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.\textsuperscript{33}

\textsuperscript{28} Art.29 Data Protection Working Party, \textit{Opinion 02/2013 on apps on smart devices}, \textit{ibid} at 22.
\textsuperscript{29} Art.26(1), GDPR.
\textsuperscript{30} Art.29 Data Protection Working Party, \textit{Opinion 02/2013 on apps on smart devices}, \textit{supra} n.27 at 23-24.
\textsuperscript{31} Art.2(c) and Art.9(1) and (2), Directive 2002/58/EC
\textsuperscript{32} Art.4(1), GDPR.
\textsuperscript{33} Art.4(6), GDPR.
Prior consultation. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. 34

Privacy. The ability of an individual to be left alone, out of public view. Privacy covers issues relating to the protection of an individual’s personal space, so a possible interference must have a legal basis, having to be “in accordance with law”, as stated in Article 8 of the ECHR. 35

Privacy by default. According to the GDPR the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed (e.g. minimization). That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 36

Privacy by design. According to the GDPR, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymization (see definition below), which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing. 37

Processor agreement. Processing via a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, also respecting the same obligation to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. 38

Profiling. Any form of automated processing of personal data using data to evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements. 39

34 Art.36(1), GDPR.
35 “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.”, Art.8, Charter of Fundamental Rights of the European Union, 2012/C 326/02.
36 Art.25(2), GDPR.
37 Art.25(1), GDPR.
38 Art.28(3), GDPR.
39 Recital 71 and Art.22, GDPR.
Pseudonymisation. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.\(^{40}\)

**R –**

**Right of access.** The data subject is entitled to confirmation from the data controller, without constraint, at reasonable intervals and without excessive delay or expense, as to whether or not data relating to him/her are being processed and to be provided with information as to the purposes of the processing, the categories of data concerned, the recipients or categories of recipients to whom the data have been or will be disclosed, and the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. Moreover, the data controller must communicate to him/her in an intelligible form the data undergoing processing and any available information as to their source.\(^{41}\)

**Right not to be subject to a significant or automated individual decision.** The data subject has the right not to be subject to decisions that produce legal effects concerning him/her, or significantly affect him/her which are based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, creditworthiness, reliability, conduct, etc.\(^{42}\)

**Right to be forgotten (or right to erasure).** The data subject has the right to obtain from the controller the erasure from the web (i.e. the results obtained from searches made on the basis of his/her name) of data concerning him/her if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, or if the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing. This right does not require deletion of the link from the indexes of the search engine: the original information will always be accessible using other search terms or by direct access to the source.\(^{43}\) Any erasure of personal data must be communicating from the controller to each recipient to whom the personal data have been disclosed.\(^{44}\)

**Right to be informed.** The data subject has the right to be informed of the identity of the controller and of his representative, if any; about the purposes of the processing for which the data are intended; of the recipients or categories of recipients of the data; of the categories of collected data, if data are not taken from him/her; of the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission (see definition above) or suitable safeguards. The controller must also inform him/her about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right of access to, and the right to rectify, the data concerning him/her (see definition of “Information” above); the existence of the right to withdraw the consent, especially in case of processing of special categories of data; the right to lodge

\(^{40}\) Art.4(5), GDPR.

\(^{41}\) Art.15, GDPR.

\(^{42}\) Art.22, GDPR.

\(^{43}\) Art.17, GDPR.

\(^{44}\) Art.19, GDPR.
a complaint with a supervisory authority; the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved; on whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.\textsuperscript{45}

Right to data portability. The data subject has the right to receive his/her personal data which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. There are two conditions for the exercise of this right. First, the processing has to be based on a consent or on a contract and, second, it has to be carried out by automated means.\textsuperscript{46} The data subject also has the right to have the personal data transmitted directly from one controller to another, but only if it is technically feasible for the controller.\textsuperscript{47}

Right to object. The data subject has the right to object at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him/her, save where otherwise provided by national legislation, at least when his data are processed by a public authority or by a data controller relying on its legitimate interest. In such cases, the controller shall no longer process the personal data unless he demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or are required for the establishment, exercise or defence of legal claims. Moreover, the data subject has the right to object to the processing of personal data relating to him/her which the controller anticipates being processed for the purposes of direct marketing (including profiling for direct marketing purposes). Where personal data are processed for scientific or historical research purposes or statistical purposes the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.\textsuperscript{48}

Right to rectification. The data subject has the right to have his/her personal data rectified or erased, in particular where the data are incomplete or inaccurate. The data controller also has to notify third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out.\textsuperscript{49}

Right to restriction of the processing. Data which are incomplete, inaccurate, stored in a way incompatible with the legitimate purposes pursued by the controller or no longer needed by the controller for the purposes of the processing, but required by the data subject for the establishment, exercise or defence of legal claims, can be frozen by the controller for a specific period of time, permitting access to the data blocked only to competent people/authorities, for purposes of proof, or with the data subject’s consent, or for the protection of the rights of a third party.\textsuperscript{50} During the period of validity of Directive 95/46/EC, this kind of right was also known as “right to block”, that is when the data subject blocks the processing of his/her personal data if it does not comply with applicable data protection law, in particular because of the incomplete or inaccurate nature of the

\textsuperscript{45} Art.12, GDPR.
\textsuperscript{46} Art.20(1), GDPR.
\textsuperscript{47} Art.20(3), GDPR.
\textsuperscript{48} Art.21, GDPR.
\textsuperscript{49} Art.16 and 19, GDPR.
\textsuperscript{50} Art.18, GDPR.
data\textsuperscript{51} (see below “Right to rectify/erase the data”). Any restriction of the processing must be communicated by the controller to each recipient to whom the personal data have been disclosed.\textsuperscript{52}

**S**

Special categories of data. Any data revealing, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health, sex life or genetic data and biometric data.\textsuperscript{53}

Security of the processing. The data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art (SOTA) – i.e. the available technology – and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected – e.g. through pseudonymization techniques (see definition above) or encryption. Moreover, the data controller must ensure that personal data can be accessed only by authorised personnel for legally authorised purposes and the implementation of a security policy with respect to the processing of personal data\textsuperscript{54} (see above “Privacy by design”, “Privacy by default”, “Processors agreement”).

Standard data protection clauses. These are standard contractual clauses that offer sufficient safeguards as required by Article 44 of the GDPR, in terms of protection of the privacy/data protection and fundamental rights and freedoms of individuals, and as regards the exercise of the corresponding rights. They can be adopted by the Commission or by a supervisory authority and approved by the Commission as “appropriate safeguards” that substitute for the lack of an “adequacy decision” for data transfers (see definition of “Adequacy decision” above).\textsuperscript{55}

**T**

Third party. Any natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.\textsuperscript{56}

Traffic data. Any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. It must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication and its processing must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.\textsuperscript{57}

\textsuperscript{51} Art.12(b), Directive 95/46/EC
\textsuperscript{52} Art.19, GDPR.
\textsuperscript{53} Art.9, GDPR.
\textsuperscript{54} Art.32, GDPR.
\textsuperscript{55} Art.46, GDPR.
\textsuperscript{56} Art.4(10), GDPR.
\textsuperscript{57} Art.2(b) and Art.6(1)(5), Directive 2002/58/EC
Trans or Cross-border processing. Means either: processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or processing which takes place in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.58

58 Art.4(23), GDPR.
Table of Contents

1. INTRODUCTION ............................................................................................................................. 21
   1.1 PURPOSE AND SCOPE OF WP2 .................................................................................................. 21
   1.2 PURPOSE AND SCOPE OF T2.1 ............................................................................................... 21
   1.3 PURPOSE AND SCOPE OF THE CURRENT DOCUMENT (D2.1) ........................................ 21

2. PRIVACY, PERSONAL DATA PROTECTION AND DATA OWNERSHIP ........................................... 23

3. INTERNATIONAL STANDARDS .......................................................................................................... 25
   3.1 INTRODUCTION ........................................................................................................................ 25
   3.2 UNITED NATIONS (UN) ........................................................................................................... 29
   3.3 ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD) ........... 32
   3.4 COUNCIL OF EUROPE (CoE) .................................................................................................. 36
   3.5 OTHER INTERNATIONAL ORGANISATIONS ......................................................................... 42
      3.5.1 World Trade Organisation (WTO) .................................................................................... 42
      3.5.2 The International Telecommunication Union (ITU) ....................................................... 44
   3.6 CONCLUSIONS ............................................................................................................................ 47

4. PRIVACY, PERSONAL DATA PROTECTION AND DATA OWNERSHIP ........................................... 48
   4.1 INTRODUCTION ........................................................................................................................ 48
   4.2 PRE 2018: EXISTING NORMS ............................................................................................... 51
   4.3 POST 2018: NEW NORMS ...................................................................................................... 52
   4.4 EUROPEAN CONVENTION ON HUMAN RIGHTS (ECHR) .................................................... 52
   4.5 CONCLUSIONS ............................................................................................................................ 53

5. NON-EUROPEAN PRIVACY AND PERSONAL DATA PROTECTION NORMS .................................... 55
   5.1 COMMON LAW JURISDICTIONS .............................................................................................. 55
      5.1.1 United States ...................................................................................................................... 56
      5.1.2 Canada .............................................................................................................................. 60
   5.2 LATIN AMERICA ...................................................................................................................... 63
   5.3 APEC PRIVACY FRAMEWORK ............................................................................................... 66
   5.4 ECOWAS PRIVACY FRAMEWORK ......................................................................................... 68
   5.5 OTHER KEY JURISDICTIONS ................................................................................................. 69
      5.5.1 China (PRC) ....................................................................................................................... 69
      5.5.2 India ................................................................................................................................... 71
      5.5.3 Russia ................................................................................................................................ 72
   5.6 CONCLUSIONS ............................................................................................................................ 73

6. SYNTHETIC LIST OF PERSONAL DATA PROTECTION AND PRIVACY OBLIGATIONS .................... 74
   6.1 ASSESSING THE KEY INTERNATIONAL PRINCIPLES AND NORMS ...................................... 74
      6.1.1 Suggested Third Generation ‘core’ Principles of relevance to the UPRAAM ....................... 76
   6.2 LIST OF DETAILED OBLIGATIONS ......................................................................................... 78
      6.2.1 Obligations premised on the EU Framework ...................................................................... 78
         6.2.1.1 End-user information .................................................................................................... 78
         6.2.1.2 Data collection .............................................................................................................. 80
         6.2.1.3 Data management ....................................................................................................... 82
         6.2.1.4 Data processing ......................................................................................................... 83
      6.3 SYNTHETIC MATRIZ ................................................................................................................ 87

Obligations premised on the EU Framework

---

Deliverable D2.1 Legal framework analysis report

18
6.3.1 The Perspective of an End-User.................................................................................. 89
6.3.2 The Perspective of an SME ..................................................................................... 91

7. SUMMARY AND CONCLUSION.................................................................................... 94

8. LIST OF REFERENCES .................................................................................................... 96
8.1 Publications of International Organisations............................................................... 96
8.2 State Publications......................................................................................................... 98
8.3 Academic, Corporate and NGO Publications.............................................................. 98
List of Tables

Table 1: US Fair Information Principles vs OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ................................................................. 26
Table 2: Uptake of FIPS as contemporary data protection principles ........................................ 28
Table 3: Synthetic List of Obligations ...................................................................................... 87
Table 4: Obligations: The perspective of an end-user .............................................................. 90
Table 5: Obligations: The perspective of an SME ................................................................. 92
1. Introduction

This deliverable is produced in the context of the Horizon 2020 (H2020) European Research project Privacy Flag.

1.1 Purpose and Scope of WP2

This deliverable is linked to the task T2.1 within work package 2 (WP2) of the project. WP2 is focused on Privacy risks analysis and modelling. WP2 will research the privacy-related risks (legal, technical and societal) and design the privacy risk analytical framework, including the UPRAAM and in depth risk analysis process.

1.2 Purpose and Scope of T2.1

T2.1 will analyse existing legal frameworks with a focus on European and international norms related to personal data protection, privacy and data ownership. The European Data Protection Directive (DPD) and its successor the General Data Protection Regulation (GDPR) will be addressed together with the EU’s fundamental rights and other EU privacy legislation, as well as international law-related obligations. T2.1 will analyse and detail the legal requirements for the Privacy Flag project from different sources. It will produce a list of key privacy and data protection principles adopted in the European Union and associated countries. The list will be reviewed and updated during the duration of WP2, taking into account the measures put into place under the proposed EU data reform package as they come into force. It will detail clearly and concisely legal requirements that flow from these principles to be supported by the platform, also taking into account legal and policy guidance applied to the concepts of privacy by design, privacy enhancing technology and the Internet of Things. Finally, T2.1 will compile and provide a synthetic list of legal requirements in terms of privacy, personal data protection and data ownership to support the tasks T2.3 and T3.3 implementation, and to serve as a common reference document for the other WP developments, as well as for the dissemination work.\(^5\)

1.3 Purpose and Scope of the current document (D2.1)

This deliverable is focused around doctrinal/library research which identifies and categorises the:

- personal data protection and privacy obligations and norms that have been developed in key national and supra-national jurisdictions, and which play a primary role in influencing international governmental and commercial practices;

obligations and norms which have developed and promoted by means of international Guidelines, Agreements and Conventions.

From that research, a set of clear and concise legal requirements is developed resulting in a synthesis of the legal risks that the Privacy Flag project will address.
2. Privacy, Personal data protection and Data ownership

Developing the proposed synthesis of legal requirements in terms of privacy, personal data protection and data ownership requires a brief evaluation of these concepts in the context of the identified Privacy Flag project environment. Contemporary popular accounts (e.g. in the media) discussing the processing of personally identifying information (PII) in digital environments can often confuse and conflate these concepts; and the general public, while often having a basic understanding of elements of privacy and data protection law, generally have a limited grasp of the wider legal implications attendant upon the processing of PII. Matters are complicated further at the supra-national (e.g. EU) and international levels because of significant disparities between national interpretations as regards the need for, and the extent of the application of, particular forms of privacy and personal data protection rights; and the degree to which the exercise of those rights should be permitted to influence the ability of state and corporate organisations to engage in methods of processing PII that further public or private actions and goals.

From a legal perspective, however, the three concepts are distinct, even if their precise import may vary across jurisdictions. Considered from an EU perspective, for example:

- the right to privacy, as identified in Art.7 Charter of Fundamental Rights of the European Union (CFREU) and Art.8 European Convention on Human Rights (ECHR), provides a qualified (i.e. subject to certain restrictions that are “in accordance with law” and “necessary in a democratic society”) negative right to be free of the “interference by a public authority”;\(^\text{60}\)

- the right to personal data protection, as identified in Art.8 CFREU, protects personal data via a qualified (i.e. subject to certain defined exemptions) set of rights and principles for personal data processing, such as the specific purposes and consent of the person concerned, without differentiating between data held in the public or private sector;\(^\text{61}\)

- the ability to exercise ownership over data (including personal data), in terms of control of the ability to access, create, modify, package, derive benefit from, sell, or remove data but also the right to assign such access privileges to third parties, where such ownership rights may be protected by laws of confidentiality and/or intellectual property rights,\(^\text{62}\) e.g. the EU Database right, but where those protections are, at the same time, qualified by both privacy and personal data protection laws.

---

\(^{60}\) And, arguably, a positive right to expect the State to adopt measures “designed to secure respect for private life even in the sphere of the relations of individuals between themselves”, X & Y _v_ Netherlands (1985) 8 EHHR 235.


Thus, with regard to personal data processed within the Privacy Flag environment, there may be considerable interplay between these legal factors, and this will impact upon the roles, rights and responsibilities of the parties with legal interests in that data.
3. International Standards

3.1 Introduction

While generalist international organisations, such as the United Nations (UN), Organisation for Economic Cooperation and Development (OECD), and Council of Europe (CoE), have played, and continue to play, some part in developing, or consolidating, normative rules or guidelines for privacy and personal data protection, it is arguable that the majority of their influential interventions had taken place by the closing decades of the last century. Since then, the dominant forces behind the continuing evolution of those norms and guidelines appear to be the major world trading blocs, such as the European Union (EU), the United States (US) and Asia-Pacific Economic Cooperation Forum (APEC).

Even in the early days, developments such as the passage of the first data protection law in Hesse, Germany in 1970, and the creation of the Fair Information Practices (FIPs) principles (which remain the primary underpinning of most current data protection laws) in the US in 1973, appeared to owe little debt to any recognisable international standards. Instead, those early initiatives appeared to emerge from a set of concerns that remain recognisable today:

“The involvement of nearly all ... citizens, the storage of especially sensitive data ..., and the databank’s capacity to exploit information for different purposes triggered demands that the Government investigate the risks of a permanent surveillance of citizens.”

and,

“Tensions among interests in efficiency, law enforcement, cost, access to knowledge and freedom of information, federalism, the vagueness of the term “privacy,” eroding practical obscurity of public records, accountability, pragmatic system design, limitations of anonymization and the problem of re-identification, fraud and risk, the incredible complexity in the provision of benefits, the needs of a large and complex administrative state, centralization versus devolved systems, and individual rights...”

64 Hessisches Datenschutzgesetz of 7 October 1970 (HDSG), GVBl. I, 625.
67 Hoofnagle, C.J. Archive of the Meetings of the Secretary’s Advisory Committee on Automated Personal Data Systems (SACAPDS): The Origin of Fair information Practices. Berkeley Center for Law & Technology.
In fact, the international standards of the 1980s and 1990s owe a great deal to these initial regional/national initiatives, both in terms of elucidating the rationales for developing privacy and personal data protection in the first place; and then in providing both the core principles on which such protection might be premised (the FIPS), and some of the key features of its administration (e.g. independent data protection authorities, establishment of organizational and technical data protection measures etc.).

By way of illustration, in a document for the Rand Corporation in 1973, Ware outlined the Fair Information Practices (FIPs) “safeguard requirements” that the US Secretary’s Advisory Committee on Automated Personal Data Systems had devised. It is instructive to compare how these map to modern privacy and personal data protection requirements, as illustrated in Tables 1 & 2 below.

Table 1: US Fair Information Principles vs OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

<table>
<thead>
<tr>
<th>FIPS “safeguard requirements”</th>
<th>OECD Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>An organization maintaining an administrative personal data system shall:</td>
<td></td>
</tr>
<tr>
<td>identify one person immediately responsible for the system,</td>
<td>Accountability Principle</td>
</tr>
<tr>
<td>take affirmative action to inform each of its employees about the safeguard requirements and rules and procedures governing the conduct of the system,</td>
<td>Security Safeguards Principle</td>
</tr>
<tr>
<td>specify penalties to be applied to any employees who violate the safeguard,</td>
<td></td>
</tr>
<tr>
<td>take reasonable precautions to protect data in the system from anticipated threats or hazards to the security of the system,</td>
<td></td>
</tr>
<tr>
<td>make no transfer of identifiable personal data to another system unless such other system also fulfils the safeguard requirements, etc.</td>
<td>Adequacy Principle No OECD Equivalent</td>
</tr>
<tr>
<td>inform an individual when asked</td>
<td>Collection Limitation Principle</td>
</tr>
</tbody>
</table>

68 See also Datalagen 1973 SFS 289 (Sweden, 1973); Bundesdatenschutzgesetz (Germany, 1977); Loi n8 78-17 relative a l’informatique, aux fichiers et aux libertes (France, 1978); Lov om offentlige myndigheders registre (Denmark, 1978); Lov om personregistre mm av 9 juni 1978 nr 48 (Norway 1978); Bundesgesetz über den Schutz personenbezogener Daten (Austria, 1978); and Loi reglementant l'utilisation des données nominatives dans les traitements informatiques (Luxembourg, 1979).

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Article/Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>To supply personal data whether he is legally required or may refuse to</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>supply the data requested</td>
<td>Principle Art. 7 &amp; 9</td>
</tr>
<tr>
<td>Inform an individual upon request whether he is the subject of data in</td>
<td>Openness Principle</td>
</tr>
<tr>
<td>the system and, if so, make such data fully available to him,</td>
<td>Art. 12</td>
</tr>
<tr>
<td>Assure that no use of individually identifiable data is made that is not</td>
<td>Use Limitation Principle</td>
</tr>
<tr>
<td>within the stated purposes of the system,</td>
<td>Art. 10</td>
</tr>
<tr>
<td>Inform an individual upon request about the uses made of data about him</td>
<td>Openness Principle</td>
</tr>
<tr>
<td>including the identity of all persons and organizations involved and</td>
<td>Art. 12</td>
</tr>
<tr>
<td>their relations with the system,</td>
<td></td>
</tr>
<tr>
<td>Assure that no data about an individual are made available in response</td>
<td>Use Limitation Principle</td>
</tr>
<tr>
<td>to a demand for data by means of compulsory legal process unless the</td>
<td>Art. 10</td>
</tr>
<tr>
<td>individual to whom the data pertains has been notified of the demand,</td>
<td></td>
</tr>
<tr>
<td>Maintain procedures that allow an individual who is the subject of data</td>
<td>Individual Participation</td>
</tr>
<tr>
<td>in the system to contest their accuracy, completeness, pertinence, and</td>
<td>Principle Data Quality</td>
</tr>
<tr>
<td>the necessity for retaining them, that permit data to be corrected or</td>
<td>Principle Arts. 8 &amp; 13</td>
</tr>
<tr>
<td>amended when the individual so requests, and assure when there is</td>
<td></td>
</tr>
<tr>
<td>disagreement that the individual's claim is noted and included in any</td>
<td></td>
</tr>
<tr>
<td>subsequent disclosure or dissemination of the disputed data.</td>
<td></td>
</tr>
</tbody>
</table>

Any organization maintaining an administrative automated personal data system must give public notice of the existence and character of the system once each year.

Any organization "proposing to establish a new system or to enlarge an existing system shall give public notice long enough in advance to assure individuals
Table 2: Uptake of FIPS as contemporary data protection principles

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Limitation Principle</td>
<td>s.7</td>
<td>Art. 5(a),(e)</td>
<td>Art. 6(1)(a),(e)</td>
<td>Principle 1, 5</td>
</tr>
<tr>
<td>Purpose Specification Principle</td>
<td>s.9</td>
<td>Art.5(b)</td>
<td>Art. 6(1)(b)</td>
<td>Principle 2</td>
</tr>
<tr>
<td>Use Limitation Principle</td>
<td>s.10</td>
<td>Art. 5(b)</td>
<td>Art. 6(1)(b)</td>
<td>Principle 1</td>
</tr>
<tr>
<td>Data Quality Principle</td>
<td>s.8</td>
<td>Art. 5(c-d)</td>
<td>Art. 6(1)(c-e)</td>
<td>Principles 3-4</td>
</tr>
<tr>
<td>Security Safeguards Principle</td>
<td>s.11</td>
<td>Art.7</td>
<td>Art. 17</td>
<td>Principle 7</td>
</tr>
<tr>
<td>Openness Principle</td>
<td>s.12</td>
<td>Art.8(a)</td>
<td>Arts.10-11,18-19</td>
<td>s.16-24</td>
</tr>
<tr>
<td>Individual Participation Principle</td>
<td>s.13</td>
<td>Art.8(b-d)</td>
<td>Art.12</td>
<td>Principle 6, s.7-14</td>
</tr>
<tr>
<td>Accountability Principle</td>
<td>s.14</td>
<td>Art.10</td>
<td>Art. 6(2), 18-19</td>
<td>s.5, s.16-24</td>
</tr>
<tr>
<td>Adequacy/Equivalency Principle</td>
<td>s.17</td>
<td>Art.12</td>
<td>Art.25</td>
<td>Principle 8</td>
</tr>
<tr>
<td>Notification Principle</td>
<td>--</td>
<td>--</td>
<td>Art.18</td>
<td>s.17</td>
</tr>
</tbody>
</table>

The following sections will briefly examine the nature and scope of the various interventions into the privacy and personal data protection policy arena made by various international organisations, paying particular regard to recent policy updates and amendments, and identifying key principles or requirements relevant to the UPRAAM.
3.2 United Nations (UN)

The United Nations (UN) has played a relatively limited role in the development of privacy and personal data protection policy since the 1990s. The *Universal Declaration of Human Rights* (1948), Art.12 and *International Covenant on Civil and Political Rights* (1966), Art. 17 both state that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

and the International Convention on the Rights of the Child (1989), Art. 16 re-iterates this statement with specific reference to children. However, *until very recently*, the UN appears to have made little effort to take a lead in this area. Consider the following brief paragraph in the UN Human Rights Committee’s *General Comment No. 16 of 1988* which does little more than reiterate the policy position taken by the OCED and CoE earlier in the decade:

10. *The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person’s private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.*

This was followed by the publication of the UN General Assembly’s *Guidelines for the Regulation of Computerized Personal Data Files* (1990), a nonbinding guidance document to UN nations calling for national regulation, which in its choice of principles and practices very largely mirrored the then draft EU Data Protection Directive (DPD) that had been published just 3 months earlier. Then, despite the hopes of a number of commentators, there was something of a hiatus in UN interest in addressing

---


73 *Ibid*.


75 COM (90) 314 final - SYN 287 and 288, 13 September 1990.

privacy and personal data protection policy until the current decade, when issues surrounding state surveillance appear to have brought the topic back to the UN’s attention.

In 2013 General Assembly adopted Resolution A/RES/68/167, The right to privacy in the digital age, calling on the UN High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and the collection of personal data, including on a mass scale. The High Commissioner for Human Rights’ report was delivered in 2014. Whilst its primary concern remained state surveillance, it noted that:

International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. Practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.

This led, in 2015, to the UN Human Rights Council (UNHRC) adopting a resolution establishing a mandate on the right to privacy in the digital age and creating a new post of Special Rapporteur on the Right to Privacy. The mandate of the Special Rapporteur includes promoting and protecting the right to privacy through efforts including gathering information from States, the United Nations, and other stakeholders, including regional human rights mechanisms, national human rights institutions, civil society organizations, and the private sector; identifying obstacles to the right to privacy and making relevant recommendations to the UNHRC.

Shortly afterwards, the United Nations High Commissioner for Refugees (UNHCR) published its Policy on the Protection of Personal Data of Persons of Concern to UNHCR. This policy applies to all personal data held by UNHCR in relation to persons of concern to UNHCR (i.e. refugees, asylum-seekers, returnees, stateless persons as well as internally displaced people). The policy takes as its starting point the Guidelines for the Regulation of Computerized Personal Data Files, but has clearly been influenced by more recent international instruments concerning the protection of personal data and individuals’ privacy, notably in the terminology, definitions, principles and concepts it adopts, which broadly follow existing norms. The basic principles contained in the Policy are also familiar:

- legitimate and fair processing,
- purpose specification,
- necessity and proportionality,

---

79 UN High Commissioner for Refugees (UNHCR), Policy on the Protection of Personal Data of Persons of Concern to UNHCR, May 2015.
80 Ibid. Section 1.4 Terms and Definitions at 9-10.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

- accuracy,
- respect for individual rights,
- confidentiality,
- security, and
- accountability and supervision\(^{81}\)

The policy also contains requirements for breach notification\(^ {82}\), data protection impact assessments,\(^ {83}\) and adequacy requirements for 3rd party transfers.\(^ {84}\)

Overall, while the UN has not been a leader in the field of privacy and personal data protection policymaking over the last 25 years, it is clear that it and its subsidiary organs are both conversant with, and generally supportive of, the key privacy and data protection principles found in EU law.

<table>
<thead>
<tr>
<th>Requirement Flags:</th>
<th>Breach notification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data protection/privacy impact assessments</td>
</tr>
<tr>
<td><strong>Risk Issues:</strong></td>
<td>Creation of Special Rapporteur on the Right to Privacy raises the likelihood of greater UN activity in the data privacy arena.</td>
</tr>
</tbody>
</table>

| **Project Lifetime Assessed Impact** | Low. |

---

\(^{81}\) *Ibid.* Section 2.
\(^{82}\) *Ibid.* Section 4.4.
\(^{83}\) *Ibid.* Section 4.5.
\(^{84}\) *Ibid.* Section 5.
3.3 Organisation for Economic Cooperation and Development (OECD)

The OECD’s Group of Experts on Transborder Data Barriers and Privacy Protection was established in 1978 and produced the first international informational privacy guidance, the Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, which were adopted in 1980. While these Guidelines were not legally binding, they were to be highly influential on international policymaking for the next 20 years.

The OECD’s approach to the issue of privacy and data protection differed from that of the contemporaneously developed Council of Europe (CoE) Convention (see below), the latter focusing on a human rights approach and the former concerned more with facilitating international trade and economic co-operation. Both were keenly aware, however, of the potential for a clash between data protection principles and the commercial desire for the global free movement of information, including personal data, as well as the temptation for States to use data protection laws to erect trade barriers. The OECD also differed from the CoE in that common law jurisdictions (e.g. Australia, Canada, New Zealand, the United Kingdom and the United States) were better placed to play a prominent role in the OECD deliberations. Certainly, much of the thinking behind the 1973 US-developed Fair Information Practices appears to be largely replicated in the 1980 iteration of the Guidelines, which focused upon 8 key principles:

- **Collection limitation**: there should be limits to the collection of personal data, and data, which should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.
- **Data quality**: personal data should be relevant to the purposes for which they are used, and should be accurate, complete and kept up-to-date.
- **Purpose specification**: the purposes for which personal data are collected should be specified and any subsequent use must be limited to that specification.
- **Use limitation**: data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the individual or b) by the authority of law.
- **Security safeguards**: data should be protected by reasonable security safeguards to protect against lost, destruction, use, modification or disclosure.
- **Openness**: there should be a general policy about openness with respect to personal data.

---


88 Ibid. at p.282.

89 Ibid. at p.274. A final key difference is that the Convention is clearly aimed at automated processing, whilst the language of the Guidelines is not restricted to computerized systems. However, both appear capable of allowing their principles to be extended to manual systems, or restricted to computerized systems.
**Individual participation**: an individual should have the right to find out information about their data and to have incorrect data erased or rectified.

**Accountability**: a data controller is accountable for complying with these measures.

The 1980 Guidelines remained in place unamended for over 30 years, and the OECD appears to have largely remained on the sidelines of privacy and data protection policymaking, with the exception of the publication of the OECD *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* in 2007, which recommended that its Member countries should co-operate across borders in the enforcement of laws protecting privacy, taking appropriate steps to:

- Improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities.
- Develop effective international mechanisms to facilitate cross-border privacy law enforcement co-operation.
- Provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards.
- Engage relevant stakeholders in discussion and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.\(^{90}\)

However, revision of the Guidelines was raised in the OECD *Seoul Declaration for the Future of the Internet Economy* in 2008,\(^ {91}\) in light of “changing technologies, markets and user behaviour and the growing importance of digital identities.” This resulted in the OECD Working Party on Information, Security and Privacy creating an Expert Group in 2010-11, which reported in 2013, and proposed a number of changes to the Guidelines.\(^ {92}\) It also produced a short report outlining a number of issues that were raised by the Expert Group but not fully addressed as part of the review process.\(^ {93}\)

Interestingly, although the Expert Group noted that the environment in which the Guidelines’ privacy and data protection principles were to be applied had changed radically, including changes to:

- “The volume of personal data being collected, used and stored;
- The range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- The value of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- The extent of threats to privacy;
- The number and variety of actors capable of either putting privacy at risk or protecting privacy;
- The frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate;"


Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

The global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.”

The changes proposed did not include any changes to the 8 key principles or to definitions of key terms like “data controller” and “personal data”, the Expert Group noting that, in its deliberations, “no clear direction emerged as to what changes might be needed at this stage.”

The primary revisions to the guidelines took the form of:

- reinforcing the accountancy principle, by introducing the concept of a ‘privacy management programme’;
- reinforcing the security safeguards principle, by introducing requirement for data security breach notification;
- making explicit the need for Member countries to establish and maintain “privacy enforcement authorities”;
- simplifying and consolidating the approach to transborder flows of personal data;
- suggesting ways in which Member countries could improve national implementations, including co-ordinated governmental approaches, the adoption of complementary measures (e.g. education and awareness raising, skills development, and the promotion of privacy-protecting technical measures), provision of credentialing programmes in data protection and privacy, and addressing the behaviour of privacy actors other than data controllers, e.g. individuals;
- encouraging cross-border privacy law enforcement co-operation, and the improvement of global interoperability of privacy frameworks through international arrangements that give practical effect to the Guidelines.

Overall, the OECD has, to date, and despite both environmental pressure, and a significant degree of lobbying, been reluctant to adapt the core principles of its Guidelines – a position which has drawn some criticism, particularly from corporate-facing organisations. It has reinforced some of those principles, with the concepts of ‘data management programme’ and ‘data breach notification’ (which have existed in one form or another in a number of national jurisdictions) making their way into the Guidance. However, the issues that the Expert Group raised in its report as meriting possible further


"Current privacy challenges are likely to become more acute as the economy and society depends more heavily on broadened and innovative uses of personal information that can be more easily gathered, stored, and analysed."

95 Supra. n.93 at p.6.


97 Ibid. Ch.1, para.15(c), and Ch.2, p.26-27.

98 Ibid. Ch.1, para.19(c), and Ch.2, p.28-29.

99 Ibid. Ch.1, paras. 16-18, and Ch.2, p.29-31.

100 Ibid. Ch.1, para.19, and Ch.2, p.31-32.

101 Ibid. Ch.1, para.20-21, and Ch.2, p.33-34.

study suggest that a more critical evaluation of the value and scope of the 8 principles may be on the cards in the near future.103

<table>
<thead>
<tr>
<th>Content Flags:</th>
<th>Data management programme</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data breach notification</td>
</tr>
</tbody>
</table>

| Risk Issues:       | Continuing review of the OECD Principles by T-PD |

| Project Lifetime Assessed Impact | Low. |

3.4 Council of Europe (CoE)

The first (and currently, only) legally binding international instrument adopted in the field of data protection emerged from the Council of Europe (CoE). The CoE was by disposition a human rights-oriented organisation, it was also more European-focused than the OECD, and thus the influence of common law jurisdictions was more muted. Referencing its earlier Convention on Human Rights, Art.8 the CoE had adopted two early Resolutions in 1973 and 1974, on "the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector", and on "the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector", respectively. These recommendations to its member states contained similar principles to those of the US FIPs, including principles pertaining to collection limitation, data quality, purpose specification, use limitation and security safeguards, and were precursors to the comprehensive Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

The Convention itself went considerably further than those initial recommendations, requiring contracting Parties to take necessary measures in domestic law to give effect to the data protection basic principles, and applying a uniform approach to data processing across the public and private sectors. It adopted the existing US FIPs approach, but permitted derogations from those principles only in specific circumstances, provided by national law. Exceptions, therefore, had to constitute necessary measures in a democratic society, “in the interests of protecting state security, public safety, monetary interests or the suppression of criminal offences or the protection of the data subject or the rights and freedoms of others.” It also introduced the notion that certain types of data, or “sensitive data”, such as racial origin, political opinions, religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions should require additional protection, and expanded the concept of data security, beyond unauthorised access, alteration or dissemination, to cover accidental or unauthorised destruction or accidental loss. These features have become key elements of the data protection regime in the EU.

An element absent from the Convention, however, was the notion of a supervisory authority – the contacting Parties had to provide a legal regime and legal remedies, but the nascent ‘data subject’ could be left to tackle the uses and abuses of their personal data on their own. This was addressed, in 2001, by means of an additional protocol to Convention 108 regarding supervisory authorities and transborder data flows. The additional Protocol required contracting parties to provide for an independent

---

105 CoE, Resolution 73(22) (1973).
108 Ibid. Art.2.
109 Ibid. Art.9.
110 Ibid. Art.6.
111 Ibid. Art.7.
112 Following the adoption by the CoE of the Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede (15 June 1999), the EU itself became a party to Convention 108.
113 CoE. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No.181) (2001).
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

supervisory authority, with powers of investigation and intervention, and the power to engage in legal proceedings or at least to bring to the attention of the competent judicial authorities violations of provisions of domestic law implementing the Convention and Protocol principles.\(^{114}\) It also reinforced the requirement for equivalency/adequacy for transborder data flows, by making it a requirement from which contracting Parties might derogate only in limited circumstances,\(^{115}\) as opposed to a derogation from unfettered trans-border data flows.\(^{116}\)

Post 2001, the role of Convention 108 has, perhaps, been overshadowed somewhat by the EU Data Protection Directive (DPD),\(^{117}\) in terms of its influence on both regional and global data protection developments. That said, it retains a unique position as a binding international legal instrument, and one that is undoubtedly less prescriptive than the DPD (and certainly more so than its imminent replacement, the EU General Data Protection Regulation (GDPR)\(^{118}\)).

Reform of the Convention began in 2010, with a number of reports suggesting potential areas for reform.\(^{119}\) This resulted in an intergovernmental committee (the Ad hoc Committee on data protection) adopting a proposal for the modernisation of the Convention in 2014. However, final adoption of an amended Convention by the Council of Ministers has been delayed,\(^{120}\) in part to ensure that it is consistent with the new EU GDPR and Police Data Directive (PDD).\(^{121}\)

There is increasing interaction between the Convention and the European Union framework,\(^{122}\) reflected in the draft Explanatory report of the modernised version of Convention 108,\(^{123}\) and in the

---

114 Ibid. Art.1.
115 Ibid. Art.2.
118 Regulation 2016/679/EU of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1-88.
preamble to the Data Protection Regulation, which makes accession to the Convention an element to be taken into account by the Commission when making adequacy decisions.\(^{124}\) It is noted, however, that accession to the Convention is currently permitted after the Consultative Committee on Convention 108 (T-PD) has reviewed the constitutional provisions and the data privacy legislation in the candidate countries against the provisions of Convention 108 and the Additional Protocol. This is not as stringent a process as EU adequacy assessments, which look beyond the legislation to how those laws are utilised in administrative and enforcement practice. The ‘modernised’ Convention looks likely to raise the standard required of existing and future member States, by requiring not just that they have “necessary legislative measures”, but also that there is “effective application” of those measures (Art.4(1)); as well as implementing more EU-like assessment (Art.19e) and review processes (Art.19h).\(^{125}\) Overall, while it is clear that Convention 108 will remain distinct in some respects from the EU framework, there will be ever closer synergies between the two.

While the ‘modernised’ Convention 108 remains in draft, a number of key changes have been identified by commentators:

\textbf{\textcircled{A}}  

The definition of ‘personal data’ is likely to be unchanged in the Convention itself, but the draft explanatory report suggests that: “An individual is not considered ‘identifiable’ if his or her identification would require unreasonable time, effort or means” and that “... ‘identifiable’ does not only refer to the individual’s civil or legal identity as such, but also to what may allow to “individualise” or single out (and thus allow to treat differently) one person among others. This “individualisation” can be done for instance by referring to him or her specifically or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, biometric or genetic data, location data, an IP address, etc.”\(^{126}\)

\textbf{\textcircled{B}}  

The concept of an ‘automated data file’ is replaced by data processing: ‘any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;’ and ‘Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria.”\(^{127}\) This latter point clearly brings manual data processing within the Convention.

\textbf{\textcircled{C}}  

The ‘modernised’ Convention will apply to “data processing subject to [a Party’s] jurisdiction in the public and private sectors”,\(^{128}\) this is a broader formulation than "in the territory of each Party”\(^{129}\) covering circumstances where, for example a private sector controller is either established on the territory and/or when activities involving the data processing are offered to a data subject in that territory.\(^{130}\)

\textbf{\textcircled{D}}  

The ‘modernised’ Convention includes a personal or household exemption for processing carried out by individuals in their private sphere for activities relating to the exercise of their private life where there are no professional or commercial grounds\(^{131}\) – but it also recognises the difficult contextual nature of the modern usage of data by individuals: ‘Whether activities are ‘purely personal or household activities’ will depend on the circumstances … when personal data is

\textsuperscript{124} Supra, n. 118, GDPR, Preamble, para. 105.
\textsuperscript{125} Supra, Greenleaf (2016), n.122.
\textsuperscript{126} Supra, n.123, draft Exp. Rep. paras. 17-18.
\textsuperscript{127} Supra, n.121, draft mod. Con. Art.2 (b), (c).
\textsuperscript{128} Ibid. draft mod. Con. Art.3(1).
\textsuperscript{130} Supra, n.123, draft Exp. Rep. para.29.
\textsuperscript{131} Supra, n.121, draft mod. Con. Art.3bis.
intentionally made available to a large number of persons or to persons obviously external to the private sphere, such as an open website on the internet, the exemption does not apply."¹³²

While the basic principles are very largely left intact,¹³³ they have been amended and added to. The key additional elements are, firstly, a requirement to demonstrate proportionality of processing in context "reflect[ing] at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake";¹³⁴ and secondly, that the processing must be "on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law."¹³⁵

The categories of special categories of data are expanded to cover amongst other things genetic and biometric data,¹³⁶ but the modernised Convention recognises the contextual problems that can arise from creating categorical lists, and while some of the categories retain their ‘red line’ status e.g. genetic data and personal data concerning offences, criminal convictions and related security measures, the others will be ‘sensitive’ only in contexts where they are being expressly processed for the sensitive element, e.g. while photographs can reveal racial origin, processing of photographs of data subjects should trigger the protection only if they were being processed to distinguish white applicants from applicants of other ethnic backgrounds, not just because they are photographs.¹³⁷

Breach notification is another new addition,¹³⁸ although a data controller is only required to notify the “competent supervisory authority” and not the data subjects themselves,¹³⁹ and the threshold is set quite high, "those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects."

The criticism that Convention 108 failed to provide adequate transparency rights to data subjects, particularly in today’s complex information environment, is addressed by the addition of requirements for data controllers to provide data subjects with particular information, whether the data is collected directly from them or via a third party, except in certain limited circumstances.¹⁴⁰ While not as prescriptive as the EU data protection regime - there is no set moment for providing the information – this clearly moves the Convention closer to the EU model.¹⁴¹

The rights of data subjects are both strengthened and expanded, again aligning the Convention more closely with the EU DP framework – a right to object to automated decision taking, a right to object to processing without demonstration of overriding legitimate grounds, a greater right of access to data.¹⁴² While there is no explicit 'right to be forgotten', it appears this is a deliberate move on the part of the drafters, to avoid the controversy that has surrounded that measure in the EU General DP Regulation. de Terwange suggests that the issue was seen mainly as one affecting social networks, and has been left to be addressed in that context.¹⁴³ If that is true, then

¹³² Supra, n.123, draft Exp. Rep. para.31-32.
¹³³ Supra, n.121, draft mod. Con. Art.5. See also de Terwangne supra, n.122 at 122.
¹³⁵ Ibid, Art.5(2).
¹³⁶ Ibid, Art.6(1).
¹³⁷ Ibid, Art.6(2).
¹³⁸ Ibid, Art.7(2).
¹⁴⁰ Supra, n.121, draft mod. Con. Art.7bis.
¹⁴¹ de Terwangne, supra, n.122 at 126-7.
¹⁴² Supra, n.121, draft mod. Con. Art. 8(a)-(g).
¹⁴³ de Terwangne, supra, n.122 at 124-125, referring to the ‘right to oblivion’.
this seems rather to overlook the discussion around search engines and other aggregators of ‘big data’.

Accountability is writ large in the modernised Convention, with accountability obligations placed on controllers and/or processors, and initially, it appears, also planned for product and service designers. This reflects the increasing emphasis placed on accountability in international discourse on data protection, and moves the Convention closer in emphasis and approach to the EU framework than the revised OECD Guidelines.

A requirement for independent supervisory authorities with significant investigatory and intervention powers is now directly incorporated into the Convention, rather than in a separate Protocol – a reflection of the important role that such authorities have acquired in both national and international thinking and in developing and sustaining effective dialogue between States.

Overall, while the ‘modernised’ Convention remains the subject of continuing negotiations between members of the CoE, with reservations outstanding on the part of the EU and the Russian Federation, it seems likely that the final outcome will largely reflect the present draft. If that is the case, while it is clear that Convention 108 will remain distinct in some respects from the EU framework, there will be ever closer synergies between the two. For some commentators this may not be a positive step – it may mean the modernised Convention fails the “Goldilocks test” – not being strong enough for the EU’s liking, but too strong for countries outside the EU – such commentators see the value of a third way between the strong EU GDPR and the non-binding OECD that remains flexible, but ultimately binding on the Parties to it.

If the existing Convention 108 can be seen to be part of the first generation of international data protection agreements, with EU DP Directive constituting the second generation, then the ‘modernised’ Convention very much appears to be aiming for inclusion in the third generation –

---

144 E.g. C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez, ECLI:EU:C:2014:317.
145 Supra, n.121, draft mod. Con. Art.8bis
146 de Terwangne, supra, n.122 at 126. The version of Art.8bis (3), cited by de Terwangne in 2014, does not appear to have survived into the May 2016 iteration of the draft modernised Convention.
148 Greenleaf (2013), supra, n.139 at 432.
149 Supra, n.121, draft mod. Con. Art.12bis
150 Supra, n.113, Additional Protocol (ETS No.181)
the likely components of which will be discussed in section 6.2.1 below – but with a degree of caution over controversial, or less well defined, elements of such third generation agreements, such as the ‘right to be forgotten’; and ‘difficult’ issues, such as if, when, and how to control data flows via the internet, and specifically the Web.

**Content Flags:**

| Principles: Proportionality |
| Data: genetic and biometric data |
| Data Breach notification |
| Accountability |

**Risk Issues:**

| Convention 108 modernisation work is incomplete. |

**Project Lifetime Assessed Impact**

| Low. |
3.5 Other International Organisations

3.5.1 World Trade Organisation (WTO)

Given the key role of personal data within the digital economy, and the growing importance of digital services in international trade, it is perhaps surprising that the World Trade Organisation (WTO), as the only global international organisation dealing with the rules of trade between nations, has not been more heavily involved in developing principles and standards relating to trans-border data flows. Equally, given the potential of data privacy laws to raise barriers to provision of services, or to permit nation-by-nation discrimination in access to personal data, one might expect Members of the WTO General Agreement on Trade in Services (GATS) to have raised complaints. In large part, this apparent inactivity can be attributed to the fact that the current WTO rules were negotiated as part of the Uruguay Round of negotiations in the mid-1990s, when provision of digital services was limited. The failure to reach agreement in the Doha Round (ongoing since 2001) has meant that updated rules reflecting contemporary development in digital services and transborder data flows have yet to emerge.

The position of national data protection laws under GATS seems clear. Article XIV: General Exceptions states that:

"Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:

...  

(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:

...  

(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts"

Thus, measures such as the existing EU DPD, the new EU GDPR and PDD, and national legislation based upon those measures, appear to be permissible, as an exception to the general GATS rules insofar as they are necessary, not used as a means of arbitrary or unjustifiable discrimination, or used as a disguised restriction on trade in services.\textsuperscript{155} It has been suggested, however, that the way in which the EU determines ‘adequacy’ under Art 25 EU DPD might, in the absence of a consistent approach to adequacy determinations, or inconsistent consequences of inadequacy rulings, fall foul of the ‘no arbitrary or unjustifiable discrimination’ rule.\textsuperscript{156} Equally, ad hoc measures such as the EU-US Safe Harbor Agreement/Privacy Shield might be seen to breach GATS, insofar as they hold


\textsuperscript{156} Reyes, ibid. 174-175.
“American companies to substantially different and lower standards when judging the "adequacy" of the American privacy regime than it does companies from Australia and elsewhere in the world.”

In the absence of WTO rules, data privacy developments in the international trade sphere have been confined to free trade agreements (FTAs) and cross-regional trade agreements (CRTAs), such as the 2011 Korea-US FTA (KORUS), the Trans-Pacific Partnership (TPP) and, potentially, the EU-US Transatlantic Trade and Investment Partnership (TTIP) and Trade in Services Agreement (TiSA).

Dix et al. note that US companies have been making the case that national restrictions on data flows, and requirements such as data processing localisation, may constitute a form of trade protectionism, and that the US Trade Representative has begun to seek language in FTAs and CRTAs that promotes free flow of information, and restricts ‘data protectionism’.

The notion of ‘interoperability’ of data privacy regimes is also being floated by the US in trade talks, particularly with the EU.

That said, to date, neither the US nor the EU appear to have explicitly sought to entrench their positions on data privacy internationally by means of FTAs/SRTAs. The KORUS agreement includes binding rules on cross-border data flows, but restricts any commitment to the parties endeavouring to “refrain from imposing or maintaining unnecessary barrier[s] to electronic information flows across borders,” while permitting the parties to adopt Internet restrictions consistent with the agreement's legally binding exceptions provision, which for the purpose of the chapter covering cross-border information flows, incorporates Article XIV of GATS *mutatis mutandis*. It does not attempt to define ‘necessary/unnecessary’ barriers. Where privacy is directly recognised in US FTAs, it has been in general terms, without specific mechanisms or policies for enforcing privacy standards.

The EU has also been disinclined to use FTAs to promote its own specific privacy principles or processes. In the 2011 EU-Korea FTA, with regard to data processing, the Parties are, in accordance with their commitments to protect fundamental rights and freedom of individuals (i.e. those set out in the Universal Declaration of Human Rights, the UN Guidelines for the Regulation of Computerized Personal Data Files, and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), to adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data.

Overall, it appears likely that, for the foreseeable future, the WTO is unlikely to play a significant role in either influencing the uptake of international data protection regulation, or

---


164 Dix, *supra*, n.159 at 283.

165 See e.g. *US-Panama Trade Promotion Agreement* (TPA), in force October 31, 2012. Art.14(5).

166 See e.g. *EU-South Korea Free Trade Agreement*, in force July 2011, Art.7.43.
determining/reinforcing the existing and developing obligations and norms which underpin national and regional implementations. While some commentators see a future role for the WTO in this area, others suggest that the speed with which the digital environment is developing means that neither formal international trade rules and organizations, nor new bi- or multi-lateral free trade agreements, may be as effective at reaching workable solutions as an informal "data privacy" trade network, i.e.

"a "hybrid" of public and private networks composed of [data privacy regulators] on the one hand, and private lawyers, academics, and transnational businesses on the other. It is a conceptual expansion of government networks or transgovernmental regulatory networks (TRNs). A TRN is composed of like-minded working-level professionals who share the common belief in regulatory problems and responses across state lines."167

3.5.2 The International Telecommunication Union (ITU)

The International Telecommunication Union (ITU), like the WTO, has been suggested as an appropriate entity to through which to provide both a forum for discussion of international data processing and transfer, and a means of devising international principles and rules.168 In the main, as with WTO, however, such hopes have not been realised.169 The ITU does produce a range of reports on privacy issues,170 and maintains a watching brief on privacy and data protection issues. However, its role in terms of development of policy, as opposed to standards development has, until recently, been limited.

One notable recent policy initiative, in conjunction with the EU and the Caribbean Telecommunications Union (CTU), was the HIPCAR (Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures) Project, in which teams of regional and international experts assessed existing legislation of beneficiary countries in areas relating to information society issues, including privacy and data protection, against international best practice, with the aim of achieving harmonization across the region. In 2013, the project produced an Assessment Report which identified key international privacy and data protection principles,171 and a set of Model Policy Guidelines and Legislative Texts for the Caribbean

---


169 In part this is due to resistance from the US, which does not want the ITU to become a “forum for adjudicating privacy and related concerns”. See Scola, N. Here’s how the U.S. plans to avoid a U.N. vote on the future of the Internet, The Washington Post, October 20, 2014.


Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

jurisdictions. As 95% of the funding of the HIPCAR project was provided by the EU, it is perhaps not surprising that the latter document bears a strong resemblance to the EU data protection framework.

As such, insofar as the ITU has engaged with policy development in particular regions, it has done so in the light of data privacy principles derived from the OECD Guidelines (1980), the UN Guidelines (1990), the EU DP Framework and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. The HIPCAR project identified the key principles as follows:

“Collection Limitation Principle: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date

Purpose Specification Principle: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose

Use Limitation Principle: that personal data is disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except either with the consent of the data subject; or the authority of law

Security Safeguards Principle: that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data

Openness Principle: that there should be a general policy of openness about developments, practices and policies with respect to personal data. Systems should be readily available to establish the existence and nature of personal data within an organisation, and the main purposes of their use, as well as the identity and usual residence of the data controller

Individual Participation Principle: an individual should have the right to obtain from a data controller, or otherwise confirmation of whether or not the data controller has data relating to him, be given reasons if a request made is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended

Accountability Principle: that a data controller should be accountable for complying with measures which give effect to the principles stated above.

Non-discrimination Principle: that sensitive information should not be processed, unless particular, identified conditions are met.

Limitation of Transborder Data Flows: that personal information should not be transferred from one jurisdiction to another without equal or greater protections to privacy and information protection

Supervision and Sanctions: designation of an authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth in the framework.

Power to Make Exceptions: the need, from time to time for departures from the principles referenced above may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures should be expressly specified in law which expressly states their limits and sets forth appropriate safeguards. “173

A similar project in Africa, HIPSSA,174 similarly funded by the EU and organised by the ITU, was responsible for producing the Southern African Development Community (SADC) Model Data Protection Law in 2013.175 While this project did not spell out its key principles in a separate document, the model law again demonstrates a distinctly European approach.176

<table>
<thead>
<tr>
<th>Content Flags: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Issues:</td>
</tr>
<tr>
<td>Significant recent developments in regional data protection laws</td>
</tr>
<tr>
<td>Project Lifetime Assessed Impact Low</td>
</tr>
</tbody>
</table>

The ITU recently created a new Study Group, SG20, on the Internet of Things and Smart Cities, which is now actively working on new draft recommendations related to privacy, including standards addressing privacy for the Internet of Things and smart cities. It complete the work initiated by Study Group 17 with a stronger focus on the security dimension of personal data protection.

173 HIPCAR, supra, n.171, 2.3 Key Elements of Privacy and Data Protection Frameworks
174 Harmonisation of ICT Policies in Sub-Saharan Africa (HIPSSA).
176 Possibly because the consultant who drafted the initial document, Jean-Marc Van Gyseghem, is a consultant to the CoE.
3.6 Conclusions

The above survey of international privacy and data protection standards suggests a reasonably coherent set of core principles that have been developed since the 1970s, and which are widely accepted by States, even if their implementation of those principles may vary significantly in practice. Developments since the 1990s have largely centred upon developing those principles, and the regulatory mechanisms for achieving them to address the emerging environmental contexts created by technological advances and globalisation; in particular, the expansion of personal data processing and data transfer capabilities far beyond those spheres of government and large corporate data centre processing envisaged by the drafters of the OECD Guidelines and CoE Convention. The ‘third generation’ of privacy and data protection standards demonstrate a reluctance to retreat from those core principles, even in the face of pressure from significant corporate and State interests. However, they also signal the entrenchment of what were once outlying norms, e.g. the need for an independent supervisory body with investigation and enforcement powers; and creation of a new set of normative standards centred on the concept of accountability, e.g. the use of ‘privacy by design’ methodologies and privacy impact assessments. The EU has been, and continues to be, a prime mover in this ‘third generation’ thinking. However, as transborder data flows have become of increasing economic importance, the frictions caused by inconsistencies or outright conflict between different regional and national regulatory strategies, even where nominally premised on the same core principles, have been thrown into sharper relief.
4. Privacy, Personal data protection and Data ownership

4.1 Introduction

Although data protection legislation exists in a variety of countries, on an international level there is no common agreement regarding its content. An initial convention, however, is to identify that Data Protection concerns the protection from abuse of such computerised data, and not their physical protection as the title may have implied. It is also clear that Data Protection legislation applies to personal data obtained and processed over the Internet as it does to information obtained by more conventional sources for automatic processing. Data Protection legislation, existing in most West European countries, is based on the regulation of Privacy provided by the national Constitutions and the legislation regulating confidential information. However, the Data Protection legislation per se was mainly influenced by the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981) which has set a number of principles for Data Protection. As noted above, the OECD Guidelines on the Protection of Privacy adopted in 1980, and the UN General Assembly’s Guidelines for the Regulation of Computerized Personal Data Files (1990), are the other two important legal texts on international level. Privacy legislation is traditionally based upon the Universal Declaration on Human Rights, and in most EU Member States the Data Protection legislation is based upon the principles established by the 1981 Convention.

The Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which was passed on 24 October 1995 is, equally, based on these principles and tries to harmonise legislation across the EU. The concept of Data Protection is based upon a system of national regulatory authorities which “regulate” the processing of personal data.

---

177 See, in the same vein, Decision C-101/01 Lindqvist of ECJ, 2003 I-12971.
178 EU countries and Iceland, Israel, Norway have Data Protection legislation. For the UK there exists legislation also for the special jurisdictions of Guernsey, Isle of Man and Jersey.
179 CoE, Convention, supra n.107.
180 OECD, Guidelines, supra n.85.
181 UN, Guidelines, supra n.74.
182 UN, Universal Declaration on Human Rights, Art. 12, supra n.70.
183 Directive 95/46/EC, supra n.117.
184 Granting a three year period for Member States to comply with i.e. this period has expired on 24th October 1998.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

In view of the expansion of telecommunications two more Directives have been introduced: In 2002 the e-Privacy Directive 2002/58185 and, in 2006, the Data Retention Directive 2006/24.186 Note, however that said Directive has been cancelled by the CJEU’s decision in Joined Cases C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and C-594/12 Kärntner Landesregierung.187

Data Protection in Telecommunications should be examined together with the bundle of Telecommunications Directives,188 which was later revised by Telecommunications Directive 2009/140.189 Following the European Parliament compromise of 5 November 2009, Directive 2009/140, repeats in article 1 (to become art.3a) the ambitious wording, referring to article 10190 of ECHR (freedom of expression), stating that:

“Measures taken by Member States... shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures ... liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process”.

The obscure wording of the law, however, does not answer directly the critical question: Are private entities, such as Internet Intermediaries allowed to restrict fundamental rights such as the right to access a network? Although the ECHR case-law is clear on several of the above matters, the

---

187 (not yet reported) 8 April 2014.
particular legislation has not been fully tested by courts\textsuperscript{191} while adjudicating a dispute between private entities.

However, in view of cancellation of Directive 2006/24, the discussion that follows immediately is focused only on the fate of existing data gathered by providers: Whether they will be allowed to erase them or whether they should retain them will be answered by future legislation. Regarding standard data protection issues, it is worth mentioning that the ECJ\textsuperscript{192} has accepted that the characterisation of processing of data as legitimate under the provisions of the Data Protection Directive should be performed ad hoc, no matter if it concerns an original collection of data or any subsequent transmission of such data via electronic means. An individual may assert against host intermediaries the right of objection\textsuperscript{193} if the Intermediary does not respond, the data subject may then refer the matter to the competent Data Protection Authority, who may impose a provisional suspension of the processing (of data) until the final decision.

In 2009, “Cookies” Directive 2009/136,\textsuperscript{194} has been introduced and Data Protection Authorities have published instructions for the provision of electronic consent. In the event of data protection breaches over networks, providers are obliged\textsuperscript{195} to inform, without undue delay, the Authorities and the user concerned. Providers may be relieved of this obligation if they prove that they have taken the necessary technical and organisational measures to avoid breaches “to the satisfaction of the competent Authority”. The parameters set by the original text of article 15 paragraph 2 of e-Privacy Directive 2002/58 allow to set a regime of liability for providers in case of data protection breaches. A similar system of liability may be introduced for providers for trafficking of spam mail. Some national legislations (e.g. the Greek) have introduce a regime of direct liability, following the view that by increasing compensation and similarly expanding the range of those obliged to notify breaches, providers would become more responsible. This approach coincides with the EU philosophy that “those who profit from the information revolution must respond to the public policy responsibilities that come with it”,\textsuperscript{196} in order to achieve a higher degree of confidentiality for users.

\textsuperscript{191} See for example ECJ decisions in Joined Cases C-397/01 to C-403/01, Pfeiffer et al. v. Deutsches Rotes Kreuz, Kreisverband Waldshut eV, ECR 2004 I-08835 and case C- 91/92, Paola Faccini Dori v Recreb Srl. ECR 1994 I-03325.

\textsuperscript{192} See Decision C-73/2007 Tietosuojavaltuutettu v Satakunnan Markinapörssi Oy and Satamedia Oy, Reports of Cases 2008 I-09831

\textsuperscript{193} Art. 14 of Data Protection Directive 95/46/EC.


\textsuperscript{195} See the wording of art. 3 par. 4 Directive 2009/136 and, the “identity theft” wording of Recital No. 61 of the Directive.

4.2 Pre 2018: Existing norms

Despite the above, the recitals in the Directive explicitly recognise that “Member States will be left a margin for manoeuvre ... [and] within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of this Directive, and this could have an effect on the movement of data within a Member State as well as within the Community”. Under the European Directive’s choice of law provision, a controller is subject to the law of each Member State where it is “established”. As explained in the Recitals, a Member State’s law thus applies if there is “effective and real exercise of activity through stable arrangements.” This definition of “establishment” suggests that the systematic collection of information from within any Member State using servers or other computing equipment within the Member State may be treated as an “establishment”.197 In effect, the controllers operating in the on-line environment may typically be deemed to be established in several Member States for the same on-line activity. As a result, several data protection laws may apply to various aspects of an on-line service.198 It is likely that the New Regulation (see infra) could probably shed light on the principles of the Directive relative to conflicting law.

The uniform choice of law rule that the European Directive requires will still not displace all possible territorial overlaps. Under the jurisdictional doctrine of the European Court of Justice,199 home country supervision for data protection would not preclude independent regulation of the treatment of personal information for other goals such as consumer protection.200 In addition, the European Directive does not displace any provisions of criminal law. To the extent that Member States include data protection offences within their criminal law, those criminal laws may apply to acts undertaken within the Member State regardless of the European Directive’s preferred choice of law.201

---

197 The use of cookies, for example, creates an establishment wherever the user is located since interaction with the user’s hard drive is a stable arrangement located at the site of the user that provides effective and real exercise of activity for the controller who places the cookie.

198 Notification of cookies must, for example, comply with the notice requirements of the place where the user is located, while the server’s processing must comply with the requirements of the law where the server is located.

199 See Konsumentombudsmannen (KO) v. DE Agostini (Svenska) Forlag AB, Cases C-34 to 36/95, [1997] ECR 1- (July 9, 1997).

200 For example, the crucial data protection provisions for on-line services in Germany arise under the Teleservices Data Protection Act. As such, these provisions might be applied regardless of the European Directive’s choice of law rules.

201 For example, France’s penal code criminalizes the “act of collection of data by fraudulent, unfair or illegal means, or to undertake processing of nominative information concerning physical persons who have opposed such processing, when such opposition has a legitimate basis”. French criminal law also specifies that, in the absence of an individual’s express consent, the storage of nominative information directly or indirectly revealing racial origins or political, philosophical or religious beliefs, union membership, or personal morals is a crime.
4.3 Post 2018: New norms

On 8 April 2016 the Council adopted the (New) Regulation\textsuperscript{202} and the (New) Directive\textsuperscript{203} and on 14 April 2016 they were both adopted by the European Parliament. On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018 and Directive 95/46/EC will be repealed with effect as of that date.

The (New) Regulation introduces special procedures for consent over the Internet and establishes the right to “Oblivion” (the right to be forgotten), already recognized by decision C-131/12 Google Spain of ECJ. It also contains special provisions for social networks and web 2.0. The important element is the introduction of full scale liability for data controllers: First, each controller / processor: jointly and severally liable for the entire damage. Second, each controller is directly liable, that is interpreted as “Processing must be performed according to Regulation”.

4.4 European Convention on Human Rights (ECHR)

The EU is required to treat “fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States” as general principles of Community law.\textsuperscript{204} While the EU is itself not a party to the European Convention on Human Rights (ECHR) and is not bound by rulings of the European Court of Human Rights (ECourtHR),\textsuperscript{205} all 28 EU member States are members of the CoE and parties to the ECHR, and are bound to follow the ECourtHR’s rulings.

This means that rulings of the ECHR in the areas of privacy and data protection are of clear significance to the EU data privacy regime, even if they are not binding upon the EU itself.\textsuperscript{206} For example, rulings considering the legitimate scope of an individual’s right to access to personal

\textsuperscript{202} Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

\textsuperscript{203} Directive (EU) 2016/680 of the European Parliament and of the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

\textsuperscript{204} Consolidated version of the Treaty on European Union, 2012/C 326/01, Art.6.3.

\textsuperscript{205} Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention (CETS No.: 194) Art.17 permits the EU to join the ECHR. However, despite the Treaty of Lisbon requiring the EU to accede to the ECHR (Consolidated version of the Treaty on European Union, 2012/C 326/01, Art.6.2), and the drawing up of a draft agreement for EU accession to the ECHR, the CJEU’s Opinion 2/13 on the draft agreement providing for the accession of the European Union to the ECHR, 18 December 2014, finding the agreement incompatible with EU law, has left accession in doubt.

\textsuperscript{206} See ECourtHR (2016) Factsheet – Personal data protection, ECourtHR Press Unit, April 2016.
data, the right of an individual to correction, erasure or destruction of inaccurate data, treatment and disclosure of sensitive data, and storage and use of personal data, will have implications for member State implementation of the EU DPD into national law, and for their interpretation of the EU GDPR in national practice.

Overall, the ECourtHR’s application of Art.8 ECHR relating to respect for an individual’s private and family life, home and correspondence has broadly reinforced a number of the core principles underlying the European data privacy framework. As the ECourtHR noted in S & Marper v UK:

“The protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned ... The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [I]t must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family.”

The ECourtHR has also consistently applied the principles of balance and proportionality to the application of measures by public authorities which seek to place restrictions on rights involving personal data under Art.8(2) ECHR including collection and retention of personal data, and disclosure of personal data.

4.5 Conclusions

The goal of the EU DPD was to begin the process of harmonising data privacy laws across the EU, and this has been successful to the extent that the EU has been able to agree the new GDPR in 2016. A directly applicable Regulation, even one with scope for a degree of member State interpretation/divergence, would have been unthinkable in 1990. However, this should not lead an observer to assume that there is a high degree of convergence in terms of national articulation of the DPD requirements in legislation and caselaw, in the degree and nature of national regulatory oversight, or in administrative practice within data controllers and processors. Any data protection officer (DPO) in a large European commercial entity will be able to describe the complex nature of

---

208 E.g. Rotaru v Romania (28341/95) 8 BHRC 449.
211 S & Marper, ibid. at para.103.
the EU data protection ecosystem, and the practical requirements of satisfying the legal and regulatory requirements of the 28 member States.\textsuperscript{213}

Data privacy laws in the EU are clearly premised in some measure upon a human rights foundation, even if some of the member States, such as the UK, have no obvious constitutional basis for a right of privacy, and only a relatively recent legal tradition of accepting breach of informational privacy as a cause of legal action in its own right.\textsuperscript{214} This foundation is reinforced by the incorporation of data privacy rights in the EU Charter of Fundamental Rights, which itself is influenced by and builds upon the prior and ongoing jurisprudence of the ECHR. There always has been, however, a pragmatic element to the EU data privacy legislation; harmonisation of member State laws is designed to prevent divergent legal and administrative practices from forming a barrier to the free movement of (information and) services within the Union. It can be expected that the directly applicable GDPR will continue, and probably hasten, the slow convergence of public and private sector practice across the EU. Drawing upon the common principles and norms underpinning the EU regulatory framework thus goes a significant distance towards evolving commercial practices that are practically, as well as facially, compliant with a range of national requirements, even though technical legal and regulatory minutiae will differ.

In the course of implementing the DPD, and in formulating the GDPR, the EU has adopted a highly prescriptive regulatory system governing both the collection of personal data by the government and private organizations. This approach has been criticised for being over-bureaucratic, tending towards focusing upon meeting administrative formalities rather prioritising actual privacy outcomes. This, in turn, it has been suggested, can cause organisations to develop management systems that are compliance-focused and inward-looking, rather than proactive, predictive and reflexive.\textsuperscript{215} Such criticism often notes the paradoxical impetus towards better privacy practices that a degree of regulatory uncertainty or fluidity can provide to organisations. In such circumstances, it is not enough to be able to point to compliance with fixed rules – the organisation must be able to demonstrate an ability to adapt to circumstance and context in its approach to fair and proportionate protection of individual data privacy.\textsuperscript{216} The increased importance in the GDPR of the principle of accountability, and the incorporation of mechanisms such as privacy by design and privacy impact assessments, are arguably evidence that EU policymakers and legislators have, to some degree, begun to take such criticisms on board.


\textsuperscript{216} Bamberger & Mulligan, \textit{ibid.} at 192 discussing the US situation.
5. Non-European privacy and personal data protection norms

It is far beyond the scope of this deliverable to produce a comprehensive overview of the development of personal data protection and privacy obligations and norms in all jurisdictions, although several commentators\textsuperscript{217} and organisations\textsuperscript{218} have taken it upon themselves to provide country-by-country international or regional overviews. This section will thus examine the general approaches taken by key jurisdictions and regions.

5.1 Common Law jurisdictions

It is perhaps tempting when considering the non-EU common law jurisdictions, to regard them as a monolithic whole in their approaches to both privacy and data protection. This would be an error much along the lines of assuming that all the EU member States take a similar attitude to the nature and scope of their obligations and data subjects’ rights under the EU DPD. There are undoubtedly some basic similarities: a cautious and less expansive approach to privacy laws, with data privacy rights not usually entrenched in the constitutional paradigm; a relaxed, not to say \textit{laissez faire}, approach to formal regulatory regimes; and a tendency towards preferring self-regulatory or co-regulatory solutions where possible. However, there is from the lawyers’ perspective also some truth to the old chestnut about English-speaking countries being separated (or divided) only by a common language - in this case the language of privacy regulation.

It is, however, instructive to examine the position of some of the larger non-EU common law states, not least, in the case of the US, as a means of assessing the effectiveness of a very different data privacy regulatory structure against the regulatory framework and national implementations in the EU member States. The verbal skirmishing between proponents of the EU framework and those who favour a US style framework has continued without let-up since the early discussion of the draft EU DPD. What has largely been lacking to date has been empirical evidence of the relative impact of


\textsuperscript{218} E.g. DLA Piper (2016). \textit{Data Protection Laws of the World}. (webpage); Privacy International (undated) \textit{Submissions to the UN}. (webpage).
5.1.1 United States

When it comes to discussion of data protection obligations and norms, the United States (US) is something of an ‘elephant in the room’. As noted in Section 3.1 above, the US devised what are recognised as the first Fair Information Practice principles (FIPs) in the early 1970s, and the US was represented during the drafting of both the OECD Guidelines (1980) and CoE Convention 108 (1981). However, while being happy to play a role in developing non-binding FIPs at the international level, largely to ensure that disagreements over protection of individuals’ data privacy did not become insurmountable barriers to transborder data flows, the US has always baulked at the idea that it should create its own comprehensive, consolidated Federal data protection law.

This is not because the US does not recognise the importance of the right to privacy. Despite the lack of an explicit Constitutional basis for a right to privacy, the concept of privacy in the sense of ‘the right to be let alone’ has long been accepted in principle by the US legal system as a constitutional right, if rarely enthusiastically supported in practice with regard to informational privacy, as opposed to physical and decisional privacy. Of course, where the US Constitution has been held to support determinable positive privacy rights, those rights are always exercised against either federal, or state government. Constitutional rights prevent the government from encroaching upon an individual’s (Individuals in general, American residents or American citizens) rights; they do not require the government to protect those rights against third parties. Thus, personal data held by third parties, such as commercial entities, are usually not protected unless a legislature has enacted a specific law, and even then that law may be subject to challenge for infringing the First Amendment rights of those wishing to process that data.

This is not to say that the USA lacks personal data privacy laws outside the constitutional sphere. Little could be further from the truth. Critics of the US position have been far more likely to claim that it lacks meaningful personal data privacy laws. As Rotenberg noted, US federal privacy statutes tended to arise less out of a concerted attempt to provide US citizens with a coherent personal data privacy regime, than out of a series of attempts either to fill legal lacuna that the courts had specifically refused to address or to assuage public concern arising from the use and abuse of new technologies.

In the words of Alderman and Kennedy:

“... the biggest problem with the statutory scheme is that there is no overall privacy policy behind it. As even a partial list of privacy laws indicates, they address a hodgepodge of

---

220 Bamberger & Mulligan, supra, n.213.
221 The US currently holds observer status on the Consultative Committee of Convention 108 (T-PD).
226 Privacy Act 1974, 5 USC § 552a; Video Privacy Protection Act 1988, 18 USC § 2710.
individual concerns. The federal statutory scheme most resembles a jigsaw puzzle in which the pieces do not fit. That is because the scheme was put together backwards. Rather than coming up with an overall picture and then breaking it up into smaller pieces that mesh together, Congress has been sporadically creating individual pieces of legislation that not only do not mesh neatly but also leave gaping holes.”

The most heavily regulated sector in the USA with regard to data privacy remains the government. Not only are there important constitutional controls on its ability to collect and use personal data in the law enforcement sector, but with regard to government collection and use of personal data for other purposes, most aspects of federal agency collection, maintenance, use and disclosure of personal information are regulated by the Privacy Act 1974, and subsequent amendments.

Thus, while the US legal system recognises a fundamental right of personal privacy, federal legislation has never provided a comprehensive regime for data privacy, and state coverage has always been, at best, variable. It is little surprise, therefore, that the EU found itself unable to plausibly grant the US an ‘adequacy’ decision for transborder data transfers, and recourse needed to be had to the now defunct ‘Safe Harbor’ agreement. That said, the US appears largely to have avoided significant public unrest over its failure to provide for overarching data privacy regulation and a single regulatory authority. In large part this has been as a result of two key developments in the US: first, the assumption by the Federal Trade Commission, via its consumer protection mandate, of a data privacy regulatory role focused primarily upon the issue of online commerce; second, the development of state-level security breach notification laws which, as a form of “regulation by disclosure”, provide the public with the kind of information necessary to put pressure on organisations, directly or indirectly, to improve their data security practices.

The FTC’s role found its initial expression in the negotiations surrounding the EU-US Safe Harbor Agreement in the late 1990s. As the US legal framework was clearly not in a position to meet the EU DPD Art.25 adequacy requirement, it was necessary for US firms to demonstrate that they were capable of self-regulation, but also for the US to demonstrate that there was a credible enforcement agency. In the absence of a specific data privacy supervisory authority, the US government turned to the FTC as a credible source of oversight. The Safe Harbor adequacy decision by the EU Commission thus makes specific reference to the FTC as a key component of the Agreement:

"The adequate level of protection for the transfer of data from the Community to the United States ..., should be attained if organisations comply with the safe harbour privacy principles ... the organisations should publicly disclose their privacy policies and be subject to the jurisdiction of the Federal Trade Commission (FTC) under Section 5 of the Federal

229 E.g. the Computer Matching and Privacy Protection Act 1988 (Pub. L. 100-503) amended it to establish procedural safeguards affecting agencies’ use of Privacy Act records in computerised matching programs.
231 The Federal Trade Commission (FTC) is an independent US federal agency. It has both competition and consumer protection jurisdiction across a range of sectors; a key consumer protection element is its mandate to act against “unfair and deceptive acts or practices.” See www.ftc.gov
Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce..."²³²

This gave the FTC a clear mandate to involve itself in data privacy matters. The lack of a formal US data protection regime, or particular expectations about how data privacy might be addressed allowed it considerable freedom over its remit, and great flexibility over how it interpreted the notion of ‘unfair or deceptive acts or practices’. Its approach thus differed from the traditional ‘command and control’ (i.e. legislated mandatory compliance with set rules) approach adopted elsewhere, consisting initially of dialogue with industry and public interest groups, stimulation of self-regulatory mechanisms such as certification schemes, and a push towards greater transparency of corporate privacy practices. This built links with industry and privacy advocates, raised public expectations of corporate practices, and opened those practices to media scrutiny and market pressure. It used its enforcement powers sparingly, initially focusing upon ‘deceptive practices’ like misleading privacy notices, but then broadening its scope to a wider range of issues that it defined as ‘unfair or deceptive’. In the absence of a statutory definition of ‘unfair or deceptive’ in the data privacy sphere this gave, and continues to give, the FTC regulation a high degree of flexibility, as it has a significant discretion to evolve expectations of what it is reasonable to expect corporations to provide in terms of data security, as the commercial environment, technology, or other facts change.²³³

Operating in tandem with the FTC’s regulatory strategy, the development of US state security breach notification laws has reinforced transparency of corporate privacy practices, provided ammunition to public interest groups, allowed the public to make informed decisions about whom to trust the security of their data, and given corporations a significant financial incentive to address risk factors in their operations.

“These laws expose [corporations] who fail to protect consumer data to civil liability, monetary losses, increased employee efforts, a tainted public image, and loss of business opportunities. ... These costs inevitably induce behavioral changes that result in more sound privacy policies and improved database-security safeguards...”²³⁴

While recognising the innovation inherent in a range of data privacy initiatives in the US, and noting the lessons that these may provide to more traditional data privacy regimes about the value of adopting a broader range of strategies into their regulatory toolkit, it is clear that the US approach does not yet constitute a credible alternative data privacy framework capable of meeting the EU’s adequacy requirements. The US government has shown increasing interest in creating a more comprehensive federal data privacy framework, with the White House publishing a report, Consumer

Data Privacy in a Networked World, in 2012, suggesting a ‘Consumer Privacy Bill of Rights’ that would be based on the following principles:

- **Individual Control**: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.
- **Transparency**: Consumers have a right to easily understandable and accessible information about privacy and security practices.
- **Respect for Context**: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security**: Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy**: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.
- **Focused Collection**: Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability**: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

These principles bear obvious resemblance to established data protection norms, but their scope is clearly intended to be qualified to both fit with the existing self-regulatory processes, and to avoid the legal challenges under the First Amendment that Federal laws limiting the collection and use of data often face. The remaining elements of the report suggest further use of self-regulatory mechanisms such as Codes of Conduct, which it proposes would be legally binding, but in which corporate participation would be voluntary; the provision of powers to the FTC to enforce the Consumer Privacy Bill of Rights, and the goal of improving global interoperability of data privacy rules. It is unclear both how the FTC would enforce ‘general principles that afford companies discretion in how they implement them’ and how such powers would significantly enhance the FTC’s role or alter its current activities.

The stated aim of improving global interoperability of data privacy rules has been treated with some scepticism by observers, as to date, such language on the part of the US administration has generally been diplomatic shorthand for other states relaxing their data privacy rules for the benefit of US corporations. A key test of the US’s commitment to ‘global interoperability’ will be the effectiveness of EU-US Privacy Shield agreement, approved by the Commission in February 2016, at protecting EU citizens’ rights when their data is processed by US corporations or sought by US authorities. The Privacy Shield provides greater protection for the data of EU citizens than was available under the Safe Harbor Agreement, but remains controversial and is likely to face legal challenge.

Overall, the US is unlikely to change its current stance on data privacy regulation significantly in the near future. Its influence on other nations through regional mechanisms, such as the APEC Privacy Framework, and Free Trade Agreements, (see above) appear to have had marginal effect on data privacy developments in those jurisdictions, and like China (see below), the US appears increasingly

---


236 Ibid at 2.


238 Art.29 Working Party (2016). **Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision**, WP 238, 16/EN
isolated in its stance. A key indirect influence that the US can exert in the digital environment is through industry, as US companies are dominant in many Internet-based personal information services. As the various skirmishes that Google has had with data protection regulators in the EU demonstrate, it seems likely that such services will be tailoring their internal organisation and compliance mechanisms influenced by a combination of EU hard regulation and US soft-touch regulation. It is worth noting that the two approaches need not be polar opposites, and that there may be regulatory benefits to combining their regulatory toolkits in the area of Internet regulation.

### Content Flags:

<table>
<thead>
<tr>
<th>Principle: Transparency</th>
<th>Data breach notification</th>
</tr>
</thead>
</table>

### Risk Issues:

Lack of a harmonised framework or specific national regulatory authority. Specific sectoral regulatory requirements at Federal or State level.

### Project Lifetime Assessed Impact

Low/Medium

### 5.1.2 Canada

Canada is, like the US, a federal state which has a number of specific privacy statutes (28) at federal, provincial and territorial levels that address the public, private and health sectors. It has both a federal Privacy Commissioner and provincial/territorial Privacy Commissioners. It has privacy laws covering public and private sectors. The public sector is covered by the Privacy Act 1985, while the primary federal act relating to the private sector is the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA) which applies to:

- consumer and employee personal information practices of organisations that are deemed to be a ‘federal work, undertaking or business’, such as banks, telecommunications companies, airlines, railways, and other interprovincial undertakings
- organisations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted ‘substantially similar’ legislation, and
- inter-provincial and international collection, use and disclosure of personal information.

As such PIPEDA does not provide a complete data privacy regime, in that it excludes personal data held by public bodies, both at federal and provincial level, as well as personal data held by private organisations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship. However, the EU considers the Canadian data privacy regime under PIPEDA to meet the criteria for ‘adequacy’ for the areas that it covers.

PIPEDA is based primarily upon the OECD guidelines – its key principles were derived from the Guidelines by way of the Canadian Standards Association (CSA). These can be summarised as:

#### Accountability:
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

#### Identifying Purposes:
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

---

239 Legislation in British Columbia, Alberta and Quebec has been deemed ‘substantially similar’.
Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Individual Access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

As with other common law jurisdictions, notably the UK prior to its implementation of the EU DPD, human rights considerations played a lesser role in the development of Canada’s private sector data privacy regime than concerns about international trade (a committee of consumer, business, government, labour and professional representatives developed the CSA principles on which PIPEDA is based), and ensuring consumer confidence in the information economy.

The Canadian Privacy Commissioner published a report in 2013 on reform of PIPEDA. In that document, she suggested that, amongst other things, there was a need for stronger enforcement powers, mandatory breach notification, and modification to PIPEDA’s accountability principles (including requiring proactive accountability and demonstration of compliance).

While Canada’s data privacy legislation may be viewed, on the whole, as a relatively mundane implementation of the principles in the OECD Guidelines, Canada has been a leader and innovator in developing processes to embed data privacy into public and private sector workflows through mechanisms like Privacy Impact Assessments (PIAs).

A PIA is a preparatory process which helps an organization assess privacy risks to individuals in the collection, use and disclosure of information, to foresee problems and to bring forward solutions. The aims of an organization conducting a PIA are to: conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified; to assess the impacts in terms broader than those of legal compliance, to be process rather than output-oriented, and to be systematic. The key benefits of PIAs can be summarised as: the avoidance of loss of trust and

---

enabling crowdsourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

reputation, the identification and management of risks, cost avoidance, meeting and exceeding legal requirements. 241

While Canada was probably not the first country to develop the concept of the PIA (that title should probably go to New Zealand) it has been instrumental influencing development of PIAs elsewhere, notably in the UK, with the UK Information Commissioner’s Handbook on PIAs drawing inspiration from, in particular, the Canadian federal PIA framework.242 The uptake and promotion of PIAs through the 2000s was primarily driven by the common law jurisdictions (Australia, Canada, New Zealand, UK and US).

Some interesting and innovative data privacy developments in Canada have arisen not out of the federal system, but out of the provinces, notably Ontario. The Ontario Information and Privacy Commissioner’s Office (OIPC) can make a strong claim to being the originator of the concept of ‘Privacy-by-Design’ - the concept that organizations need to build privacy directly into technology, systems and practices at the design phase, thereby ensuring the existence of privacy from the outset. Privacy by Design consists of seven key principles:

- **Proactive not Reactive; Preventative not Remedial.** Organisations should anticipate and prevent privacy invasive events before they happen, rather than waiting for privacy risks to materialize;
- **Privacy as the Default Setting.** No action should be required by individuals to maintain their privacy; it should be built into the system by default.
- **Privacy Embedded into Design.** Privacy should be an essential component of the core functionality being designed and delivered.
- **Full Functionality - Positive-Sum, not Zero-Sum:** Organisations should seek to accommodate all legitimate interests and objectives, rather than making unnecessary trade-offs.
- **End-to-End Security—Full Lifecycle Protection:** Strong security measures are essential to privacy, from start to finish of the lifecycle of data.
- **Visibility and Transparency - Keep it Open.** All stakeholders should be assured that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.
- **Respect for User Privacy - Keep it User-Centric.** Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Overall, Canada presents as a paradigmatic common law jurisdiction. While its public sector-facing privacy laws are, like that of the US, undoubtedly influenced by concerns of potential government overreach and interference in individual rights, its private sector laws show greater concern with issues such as consumer protection in order to stimulate e-commerce, and maintaining access to transborder data flows. Compared to the US, Canada tends more towards the mainstream of national data protection regimes, but the influence of US thinking on data privacy regulation is apparent. Current proposed reforms reflect contemporary international trends, with an emphasis on demonstrable accountability of data controllers and mandatory breach notification.

---


5.2 Latin America

In Latin America states, the initial approach to data protection and privacy appears to have come not via legislation, but through data protection mechanisms based on the concept of *habeas data*, a constitutional right that grants individuals access to their personal data and the right to correct inaccurate information. There are a range of views on the origins of the right, but they lie partly in European constitutional law, notably the right to information self-determination created by the German Constitutional Tribunal, and partly in CoE Convention 108. It found its first expression in the Brazilian Constitution of 1988:

LXXII – The writ of *habeas data* shall be granted:
(a) to guarantee access to information concerning the claimant stored in the records of databases of entities of the government or of a public nature and
(b) to rectify the data, unless the claimant prefers a non-public proceeding, whether judicial or administrative.

and during the 1990s similar provisions were incorporated into the constitutions of Paraguay, Peru, Argentina, Ecuador, Colombia, Panama and Honduras. The Organization of American States (OAS) describes the right as:

Habeas Data is a mechanism that provides the individual with the power to stop abuse of the individual’s personal data. In general, Habeas Data provides an individual with access to personal information in public and/or private databases, the ability to correct or update the data, the ability to ensure that sensitive data remains confidential, and allows the removal of sensitive personal data, which may damage the individual’s right to privacy.

Writing in the early 2000s, Guadamuz suggested that the *habeas data* approach constituted a “... Third Way, if you may. It does not leave privacy concerns to self-regulation schemes as the American.

---


245 *Constitution of the Federative Republic of Brazil* (1998) Title 2, Chapter 1, Article 5, LXXII.

246 Translation from Gonzalez, *supra*, n.243 at 651.
It does not create more bureaucracy as the European one. One may say that it is just right for developing countries.”

The key problems with reliance upon the habeas data approach, despite later iterations providing a more complex rights than the Brazilian model, are that:

- while in principle, it creates a private cause of action to insure compliance with constitutionally protected rights of privacy and information self-determination, which can be enforced through existing courts and procedures, in practice national constitutional principles usually required further legal rules to make them effective.
- the protection it provides is essentially an after-the-fact remedy, and the cost of making an application to judicial authorities can be off-putting to many potential applicants – for many complaints about misuse of personal data, it is taking a sledgehammer to crack a nut.
- it leaves individuals pitted against the state or private enterprise, with no data protection authority to mediate, or to set data protection standards, e.g. for security and confidentiality, for data controllers to work to and against which their actions could be measured.
- it has nothing to say about key contemporary principles such as collection limitation, data quality, purpose specification and use limitation.
- it provides little or no explicit protection for individuals in the types of circumstances made increasingly common by advances in technology and trade, such as transborder data flows.

These issues meant that states which had adopted the habeas data approach have been placed under some pressure to develop more sophisticated legal protections and administrative processes. A further driver in the development of Latin American data protection from the 2000s onwards has been a desire to obtain an ‘adequacy ruling’ from the EU Commission, given the cultural and trading ties of many Latin American states to, in particular, the Iberian EU member States. Argentina was the first Latin American state to develop a comprehensive data privacy law in 2000, and the first to obtain an adequacy ruling from the EU Commission. It has since been followed by Uruguay (2008, 2009), Mexico (2011), Peru (2011), Costa Rica (2011), Colombia (2011), Nicaragua.

---

247 Guadamuz, supra, n.243
249 Martinez-Herrera, ibid. "... the preamble to the data privacy bill currently being discussed in Colombia ... clearly states that one of the goals ... is for Colombia to be considered an “adequate protection” jurisdiction by the EU."
250 Personal Data Protection Act 25.326 (Ley 25.326 Protección de los datos personales)
252 Personal Data Protection and Habeas Data Action Act 18.331 (Ley N° 18.331 Protección de Datos Personales y Acción de Habeas Data) 2008.
254 Personal Data Protection Act 29.733 (Ley de Protección de Datos Personales) 2010.
255 Protection of the Individual Against the Processing of his Personal Data Act 8968 (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales) 2011
256 General provisions for the protection of personal data (Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales) 2012.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

(2012)\textsuperscript{257} and Dominican Republic (2013),\textsuperscript{258} although only Uruguay has obtained its adequacy ruling.\textsuperscript{259} Brazil is currently in the process of updating its data protection laws.

Overall, the picture in Latin America is mixed, with 5 types of data protection regime in existence:

- Countries with a constitutional habeas data model, possibly with some additional legislation: Brazil, Paraguay, Ecuador, Panama and Honduras.
- Countries with basic data protection laws: Chile.\textsuperscript{260}
- Countries with comprehensive data protection laws modelled on the EU pattern: Uruguay, Mexico, Costa Rica, Nicaragua, and Dominican Republic.
- Countries with a constitutional habeas data right and comprehensive data protection laws: Argentina, Colombia and Peru.
- Countries with no current comprehensive data protection legislation or habeas data constitutional rights: Bolivia, El Salvador, Guatemala, Venezuela and Cuba.

The trend, however, appears to be towards the EU ‘third generation’ model of data privacy laws, albeit with some differing elements – Nicaragua has a ‘right to oblivion’, and Costa Rica has a ten-year limitation on the retention of personal data.\textsuperscript{261} Mexico is seen by some commentators as having adopted a more APEC type approach, doubtless with its relationship with its immediate northern neighbour in mind.\textsuperscript{262} Rich suggests that, in general, the core data protection principles are reflected in most Latin American laws, but that “specific requirements, particularly with respect to cross-border, transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO) vary widely from each other and from laws in other regions of the world.”\textsuperscript{263}

The Ibero-American Data Protection Network (RIPD) created in 2003 by a consortium of the governments of Spain, Portugal, Andorra and 19 Latin American countries\textsuperscript{264} to exchange information and promote collaboration on personal data protection matters, has been influential in promoting an more uniform approach.


\textsuperscript{258} Organic Law 172-13 on the Protection of Personal Data 2013.


\textsuperscript{260} Chile has had a data privacy law since 1999, but this makes no provision for a data protection authority, does not require registration or notification and does not regulate transborder transfers of data.


\textsuperscript{262} Ibid.

\textsuperscript{263} Ibid.

\textsuperscript{264} Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Dominican Republic, Uruguay, Venezuela.
5.3 APEC Privacy Framework

The Asia-Pacific Economic Cooperation (APEC) forum is a regional group of 21 economies around the Pacific Ocean. It began life as an informal meeting of government trade officials, and remains largely a discussion forum: no treaty obligations or binding commitments are required of its participants. It produced the initial part of its Privacy Framework in 2004, focusing on domestic implementation, and the Framework was completed with a section on cross-border elements in 2005. This was followed in 2007 by an initiative involving 13 of the APEC states, the APEC Data Privacy Pathfinder. This was designed to facilitate accountable cross-border flows of personal information within the APEC region, by devising principles of how cross-border rules should work across economies, developing consultative processes for stakeholders, developing practical documents and procedures for practical application of cross-border privacy rules, discussing practical implementation and promoting education and outreach. This led, in turn, to the establishment of an APEC Cross-Border Privacy Enforcement Arrangement (CPEA) in 2010, allowing Privacy Enforcement Authorities (PEAs) to share information and provide assistance for cross-border data privacy enforcement, and the APEC Cross Border Privacy Rules System (CBPR) in 2011. The CBPR system aims to provide a transborder data transfer process whereby the privacy policies and practices of companies operating in the APEC region are assessed and certified by a Third party verifier (or “Accountability Agent”) as following a set of commonly agreed upon rules based on the APEC Privacy Framework. There is current dialogue by APEC with the EU in regard to developing interoperability between the APEC CBPR process, and the EU system of Binding Corporate Rules.

The Privacy Framework consists of 9 principles, which are largely based on the 1980 OECD Guidelines. These are:

- preventing harm to data subjects;
- provision of a notice;
- limitation on collection of personal data;

---


limit on the uses of personal information;
- individual choice over use and disclosure;
- maintaining the accuracy and integrity of personal information;
- security safeguards;
- access and correction; and
- accountability via a regulatory framework.\(^{270}\)

Most of the principles are similar to long-standing international data privacy norms (albeit the norms of the 1980s). As Greenleaf noted in 2009, those principles "are weaker than those of the European Privacy Directive, [and] of most existing data protection laws in the Asia Pacific."\(^{271}\)

The scope of the APEC principles is also narrower than many existing data privacy laws, insofar as it explicitly provides that some types of personal data (e.g. "publicly available personal information", that is, information published by the media or put into the public domain by the data subject) will be subject to minimal protection – a key difference with the EU regime, which makes no such distinction.\(^{272}\)

However, the first and last of the APEC principles are notable in their departure from those existing principles. The first APEC Privacy Framework Principle states that data protection rules should place obligations on data controllers to consider the "harm" that their processing of personal data might cause, and that remedies for data subjects should be "proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information."\(^{273}\)

As Pounder notes, this 'data controller-determined harm' approach runs entirely counter to established data privacy norms elsewhere.\(^{274}\) The ninth Principle holds controllers accountable not only for the specific measures they take to comply with the Framework Principles, but also for the information practices of data recipients, unless individual consent is obtained for the transfer. However, that accountability is limited to the exercise of 'due diligence' by the data controller and the taking of 'reasonable steps' to ensure a recipient treats the data appropriately. It seems likely that, unless 'due diligence' and reasonable steps' are interpreted carefully (perhaps with an eye towards the way that the FTC has addressed such concepts in the US), this is likely to leave a data subject with limited effective redress should their data be misused by a recipient outside their own jurisdiction.\(^{275}\)

Overall, the APEC Privacy Framework appears to provide relatively little to the list of international norms and principles of data privacy, insofar as its main goal appears to be "effectuate, rather than limit, both domestic and international transfers of personal data".\(^{276}\) It may be that the aim is to use the Privacy Framework, in conjunction with the Cross-Border Privacy Enforcement Arrangement and Cross Border Privacy Rules System, to 'ratchet up' regional


\(^{271}\) Greenleaf, supra, n.266 at 29.

\(^{272}\) Bulford, supra, n.238 at 710.

\(^{273}\) APEC Privacy Framework, Principle I: Preventing Harm, section 14.


\(^{275}\) For criticism of this principle, see Pounder, ibid. and Greenleaf, supra, n.266 at 31.

\(^{276}\) Bulford, supra, n.238 at 718.
privacy laws to higher levels, based on best regional practice and with the ultimate aim of harmonisation with EU BCRs. If that is the case, however, at present, this goal would appear to be some way off. As one commentator puts it there is a “persuasive argument ... that the EU data protection framework is increasingly becoming the global norm and that the APEC Privacy Framework fails to substantially improve on the EU principles enough to constitute a viable alternative.”

<table>
<thead>
<tr>
<th>Content Flags:</th>
<th>Principle: Harm to data subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Issues:</td>
<td>None</td>
</tr>
<tr>
<td>Impact</td>
<td>Low</td>
</tr>
</tbody>
</table>

### 5.4 ECOWAS Privacy Framework

The Economic Community of West African States (ECOWAS) is a regional group of 15 Member States established in 1975 to promote economic integration in the region. In 2010 the member States adopted the legally binding *Supplementary Act on Personal Data Protection within ECOWAS*, setting out specific criteria for legislation on data privacy and the establishment of an independent data protection authority. To date, it appears that 7 of the ECOWAS member States have implemented legislation and a further 7 have created draft legislation.

*The Supplementary Act* is clearly grounded in human rights terms, and appears strongly influenced by EU (and French) data privacy laws and norms. Bygrave indicates that, in terms of possible innovations, the Supplementary Act:

- requires ECOWAS states to apply a similar ‘adequacy’ test for transborder data transfers outside ECOWAS states as is required by the EU for transfers outside the EEA, but does not make provision for the types of derogation permitted in the EU DPD.
- while it largely follows established data privacy requirements, includes some quirks of its own, including the addition of ‘non-fraudulent’ to the usual principle of ‘fair and lawful processing’; the inclusion of ‘parentage’ and ‘genetic data’ to the categories of sensitive data; an apparently unique obligation on a data controller to ensure ‘durability’ of data (Bygrave does not appear to see the first and third of these as adding significantly to the legislation). Overall, the ECOWAS *Supplementary Act* is probably the best known of the data privacy initiatives in Africa, although there are other initiatives at an earlier stage of development, such as the ITU/EU

---

278 Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.
279 *Supplementary Act on Personal Data Protection within ECOWAS* (A/SA.1/01/10), 16 February 2010.
280 UNCTAD (2015). “ECOWAS Countries discuss harmonization of cyberlaws”, 31 March 2015 (webpage)
282 *Supplementary Act, supra*, n.279, Art. 24.
283 Ibid. Art.30.
284 Ibid. Art 45.
assisted SADC Model Law,\textsuperscript{286} and developments emerging from the East African Community (EAC) Legal Framework for Cyberlaw. The African Union passed the Convention on Cyber Security and Personal Information in 27 June 2014.\textsuperscript{287} This was signed by 53 of the 54 African States and sets forth the legal and institutional framework for the protection of personal data to be implemented by signatory states. However, the Convention will only enter into force after it has been ratified by 15 countries. The ERCOWAS privacy framework appears to fall broadly within the scope of existing international data privacy norms, albeit with a definite Franco-EU slant.

<table>
<thead>
<tr>
<th>Content Flags:</th>
<th>Adequacy without derogations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Principle: Non-fraudulent processing</td>
</tr>
<tr>
<td></td>
<td>Principle: Durability of data</td>
</tr>
<tr>
<td>Data: Parentage and Genetic data</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Issues:</th>
<th>Significant recent developments in regional data protection laws</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Lifetime Assessed Impact</td>
<td>Low</td>
</tr>
</tbody>
</table>

### 5.5 Other Key Jurisdictions

Greenleaf suggests that, at present, there are in the region of 109 countries with some form of data protection legislation, on the basis that a ‘qualifying’ country has:

> “a ‘data privacy law’ if it has one or more laws covering the most important parts of its private sector, or its national public sector, or both, and if that law provides a set of basic data privacy principles, to a standard at least approximating the minimum provided for by the OECD Guidelines or Council of Europe (CoE) Convention 108, plus some methods of officially backed enforcement (i.e. not only self-regulation). To approximate the OECD/CoE standards, a law must provide individual participation (right to access and correction), finality (additional uses and disclosures limited by the purpose of collection), security and at least 11 of the 15 OECD/CoE ‘content principles’ overall.”\textsuperscript{288}

The 3 jurisdictions chosen for survey here are significant in terms of their size of population and international influence, and run the gamut of Greenleaf’s qualification range: China is not a ‘qualifying’ country, India is (just) and Russia comfortably makes the grade.

#### 5.5.1 China (PRC)

China is a member of the APEC forum, but does not appear to be heavily involved in the developments around the APEC Privacy Framework – e.g. it did not take part in the APEC Data Privacy Pathfinder programme. This may be because China currently has no comprehensive data

\textsuperscript{286} ITU, HIPSSA - SADC Model Data Protection Law, \textit{supra}, n.175.


\textsuperscript{288} Greenleaf, G. (2015)."Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority" \textit{Privacy Laws & Business International Report}, 133: 14, fn.4. Greenleaf is at pains to note that making the list demonstrates that country meets the necessary criteria on paper, and says nothing about the effectiveness of any national data privacy regime.
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

protection legislation\(^{289}\) and no primary national regulatory authority. What data privacy-related rules there are, can be found spread between a range of sector-specific legislation, regulations and administrative guidance.\(^{290}\) Key elements include the Standing Committee of the National People’s Congress (SC-NPC) “Decision on Internet Information Protection” in 2012 and its amendment of the “Law on the Protection of Consumer Rights and Interests” in 2013,\(^{291}\) and Regulations and Guidelines promulgated by the Chinese Ministry of Industry and Information Technology (MIIT) in 2011 and 2013.\(^{292}\) While these contain references to concepts such as:

- principles of legality, legitimacy and necessity objective, methods and scope for collection and use of information - SC-NPC Decision 2012;
- personal data processing principles, collection limitations and notification, limited data breach notifications, data exports limitations - MIIT Regulations 2011;
- data exports, sensitive data, data subject access and the right to rectification – MIIT Guidelines 2013;

commentary on the scope of legal obligations arising from this patchwork suggests that clear-cut general principles and norms are difficult, if not impossible to parse. In the words of de Hert & Papakonstantinou: “Among the biggest shortcomings of the Chinese data protection system [are] the lack of common definitions, the lack of the notion of individual consent, the lack of any mention to the rights of information, access and rectification, as well as the lack of a supervising state authority.” It appears from other commentators that, in addition to these lacks, one can probably add a general lack of interest in enforcement.\(^{293}\) In general, it appears that, unlike the development of CoE Convention 108 and the EU DPD where protection of human rights was a significant driver, the interest China has shown in data privacy derives primarily, if not exclusively, from concerns about developing commerce, i.e. in developing consumer trust in e-commerce. In this treatment of privacy as a consumer protection issue, it comes closer to elements of the US approach (via the FTC) to digital privacy protection, of any of the current approaches.

<table>
<thead>
<tr>
<th>Content Flags:</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Issues:</td>
<td>Lack of clear data privacy regime/regulator</td>
</tr>
<tr>
<td></td>
<td>Unpredictability of changes</td>
</tr>
<tr>
<td>Project Lifetime Assessed</td>
<td>N/A</td>
</tr>
</tbody>
</table>

\(^{289}\) A draft Personal Information Protection Act was apparently considered in the mid to late 2000s, but not passed into law.


\(^{291}\) de Hert, P & Papakonstantinou, V. *ibid.* at 19, 21.


5.5.2 India

India currently has no comprehensive data protection legislation and no primary national regulatory authority;294 it is also not party to any specific data protection agreement or convention, although it is a party to more general human rights instruments, such as the UN Universal Declaration of Human Rights and International Covenant on Civil and Political Rights which recognise privacy rights. Several draft data privacy bills have been proposed in recent years,295 the latest being debated in 2014.296 The latter bill aimed to create a Data Protection Authority of India and would, according to Greenleaf, have given India a set of National Privacy Principles which went "considerably beyond the OECD Guidelines and ... closer to the EU data protection Directive and in some cases stronger than current European principles",297 although the bill appeared to restrict those rights to residents of India. As matters stand, however, such data protection law as there is, is contained in the Information Technology Act 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011) made under s.43A IT Act, which create a quasi-data protection framework which Greenleaf dismisses as:

"superficially resembling a data protection law, ... they have crippling deficiencies and ambiguities ... half of the Rules only apply to a very restrictive definition of ‘sensitive personal data’, and not to other personal data; half of them do not impose obligations in relation to data subjects per se, but only to ‘the provider of the information’; and it is questionable whether and when consumers (data subjects) are given a right of civil action."298

It appears from discussion of the draft Bills that India is likely, if it manages to pass data protection legislation, to produce a framework that resembles the principles and norms in CoE Convention 108 and the Additional Protocol 181, with some elements similar to the EU DPD. India’s current regime was the subject of an adequacy report commissioned by the EU in 2010 and was found wanting:299 it is clear that the Indian authorities are aiming for any new regime to be a candidate for adequacy.

---

297 Ibid.
298 Greenleaf, supra, n.295.
5.5.3 Russia

Russia has signed and ratified both the ECHR and CoE Convention 108, and the Russian Constitution provides for both the right to privacy and the right to protection of personal data.\(^{300}\) Federal Law No. 152-FZ on Personal Data 2006, in conjunction with other legislation,\(^{301}\) is seen as broadly covering the same ground as the EU DPD, although Russian terminology differs, e.g. the laws do not contain the concepts of "data controller" and "data processor".\(^{302}\) There is also a primary national regulatory authority, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).

Two notable recent additions to Russian law are the Federal Data Localisation Law,\(^{303}\) and the Federal Delisting or 'Right to be Forgotten' Law.\(^{304}\) The primary focus of the Data Localisation Law is data operators established in Russia processing personal data in the context of that establishment. However data controllers established outside Russia are required to "record, systematize, accumulate, store, amend, update and retrieve" data using a 'primary database' physically located in Russia, if they gather such data through processes, such as websites "aimed at the territory of Russia". Data can then be transferred to 'secondary databases' external to Russia, where such transfers meet Russian cross-border transfer rules, and can then be processed further under the destination country's data protection law. It appears that the law applies when the data operator collects personal data directly from individuals, and not when the data operator receives personal data from third parties, and that it does not apply to processing that occurred before 1 September 2015.

The Delisting or ‘Right to be Forgotten’ Law requires operators of search engines to remove links that provide access to personal information about a data subject which is false, out-of-date, or no longer applicable to the data subject (with some exceptions, e.g. unexpired criminal records), at the data subject’s request; or, alternatively, to send the data subject a reasoned refusal. If the data subject believes the refusal to be unreasonable they can file a claim with a court for removal of the links. Of the two Laws, the former is perhaps the more controversial, as the latter would appear to largely mirror the judgement of the CJEU in Case C-131/12 Google Spain v AEPD and González.\(^{305}\)

Overall, the principles and norms underpinning the Russian data protection regime are essentially those of CoE Convention 108 and the Additional Protocol 181, although legislators are clearly cognisant of, and willing to adopt, at least some ‘third generation’ norms.


\(^{301}\) E.g. Federal Law No. 149-FZ on Information, Information Technologies and Data Protection 2006, and sectoral specific DP provision, such as Ch.14, Russian Labour Code which addresses the personal data of employees.


\(^{305}\) EU:C:2014:317
5.6 Conclusions

The international data privacy landscape has changed rapidly over the last decade, as both international organisations and states have responded to the impact of new data processing technologies and the globalisation of trade. Insofar as patterns emerge from those changes, they appear to be that the principles and norms in the OECD Guidelines and CoE Convention widely underpin national data privacy frameworks and regional agreements/guidelines, even where the protection of human rights is not a primary driver. Where countries have weak or no data privacy frameworks, the influence of those principles and norms may still be apparent in either legislative/regulatory terminology, or in particular sectoral practices.

The Art.25 ‘adequacy’ process in the EU DPD has also had a major influence on non-EEA states, encouraging them to adopt norms and practices that aim, if not to precisely mirror the EU legislation, then at least to achieve the same purposive ends. This means that in practical terms, an organisation meeting the requirements of the EU DPD will currently ensure a high level of compliance with the majority, if not all, of the current data protection regimes world-wide. Where states have no coherent or overarching data protection regime and/or lack a national data protection regulatory authority, care needs to be taken in terms of meeting specific sectoral requirements, but an organisational commitment to at least the CoE Convention 108 principles and norms should largely meet the requirements of national laws, and the expectations of their data subjects, in virtually all cases.

Traffic in data privacy innovation has not been one-way, as developments in other jurisdictions have had demonstrable effects in improving both data privacy and data security. The common law jurisdictions have led the way in developing practical solutions for embedding data privacy in public and private sector work flows (e.g. PIAs and privacy by design), and have had some success in utilising regulatory tools such as self-regulation, co-regulation, market forces through non-traditional means, such as sectoral regulators (e.g. the FTC) and data breach notification laws. The EU GDPR reflects the success of these mechanisms in allowing data privacy regulation to develop from requiring basic compliance to encouraging continual organisational reflexivity by incorporating them into the future EU data privacy framework.
6. Synthetic list of personal data protection and privacy obligations

6.1 Assessing the Key International Principles and Norms

There have been a number of attempts at defining the key principles and norms of data protection regulation on an international basis. The general conclusion appears to be that “it’s complicated”, for even where states begin from a common normative or legal base, such as the OECD Guidelines, the CoE Convention 108 or the EU DPD, there is a tendency to diverge in terms of drafting legislation, and even greater diversity in practical administration and enforcement. This combination of legislative complexity and regulatory decision-making discretion has consistently defeated those attempting to build systems which can precisely predict the outcome of data privacy scenarios across multiple jurisdictions, or indeed, sometimes within just one. Multiply the possibilities by over 110 countries with defined data privacy laws, add nearly the same number with no laws or ‘patchwork’ laws, and take into account 2 of the world’s superpowers, China and the US, consistently refusing to engage in international dialogue on data privacy on anything but their own terms, and it is a wonder that problems like the EU/US data transfer difficulties post-Schrems don’t occur on a more regular basis.

Yet, when reviewing the previous 4 sections of this document, several issues become apparent:

- The diverse global stage across which data privacy principles have been tested for the last 30-40 years, the variety of national and regional ‘experiments’, and the degree of public, academic, corporate, and governmental engagement and cross-fertilisation, has produced valuable evidence about the successes and failures of particular modes of regulation in particular circumstances. For example:

- The EU model of top-down regulation can be criticised for obstructing corporate innovation in data privacy, by focusing the attention of organisations upon compliance with particular regulatory requirements rather than encouraging them to seek out and address non-compliance-related weaknesses or to think about data privacy issues holistically – the GDPR recognises that and draws upon developments that arose in other jurisdictions, such as privacy-by-design and privacy impact assessments, as part of a shift from a focus on compliance to a more reflexive accountability.

- The US model of self-regulation/sectoral regulation without a central data privacy regulator has demonstrated effectively that sometimes a strong regulator, in this case the FTC, is required to intercede where the invisible hand of the market fails; and that self-regulation works rather better when placed in tandem with formal legal requirements of transparency, such as breach notification laws. The fact that the FTC has been permitted to develop its mandate, and that the

---

majority of US states have been prepared to adopt breach notification laws demonstrates an understanding in US Federal and State governments of the importance of data privacy (whatever the underlying rationale), and an ability to not just tolerate, but encourage, flexible regulatory approaches.

Regardless of whether a State believes that personal data is a human rights issue, a consumer protection issue, or an international trade issue, ultimately the type of rights granted to data subjects and the obligations placed on data controllers that will most effectively achieve those objectives often turn out to be similar. While the precise formulations of the OECD Guidelines and CoE Convention may have dated, their underlying principles have demonstrated an enduring robustness in practice. Contemporary reforms of those principles have thus concentrated more on measures to encourage their incorporation into government and corporate workflows, via measures such as requirements for data management programmes, privacy-by-design and PIAs, and the promotion of accountability frameworks.

For many public and private organisations, both in the EU and elsewhere, the impact of third generation data privacy regulation and the concomitant refocusing upon accountability, is likely to be that they are going to have to adjust from thinking primarily about 'shallow' data privacy compliance, to addressing 'systemic' data privacy impacts and risks. Moving from compliance to accountability may, for example, mean that whereas it may currently be possible to meet compliance criteria easily, e.g. addressing the data subject’s right to information, by providing particular information to data subjects at a particular point in time – in other words, ‘ticking the box’, accountability might require more thought. In this example, an organisation considering this issue from an accountability perspective might need to consider questions addressing the:

- nature and value of the information - too much, too little, too complex;
- nature of the data subject(s) - Is the information or its mode of delivery ‘one-size fits’ all? Might other ways of providing it be more effective?
- Timing of delivery - is once enough?
- through to more complex issues:
  - how does the process fit with the organisation’s other data privacy processes?
  - how does the process match up to sectoral best practice, against which it might be judged?
  - how does the organisation demonstrate that it has engaged with these types of questions, and whose responsibility is it?

In the final analysis, therefore, when considering what constitutes core principles and norms from the standpoint of an EU project, one is ineluctably drawn back to the modernised CoE Convention 108, and the EU GDPR. These two documents represent the latest in contemporary thinking on the effective administration of a data privacy regime. Both draw on a global legal and regulatory heritage, reflecting lessons learned from 30 years of practice, not just in the EU, but also in jurisdictions like the US and Canada, that have successfully developed new legal mechanisms, such as breach notification, and administrative practices, such as privacy impact assessments. When such developments are incorporated into a data privacy framework like that of the EU, they encourage the development of public and private sector practices that are premised on an understanding that data privacy practice is not just a matter of simple compliance, it should be an evolving process of engagement with stakeholders inside and outside an organisation that both predicts and responds flexibly to changing environmental factors. With that in mind, the following section suggests what might be regarded as the core principles of the third generation of data privacy regulatory rules.
6.1.1 Suggested Third Generation ‘core’ Principles of relevance to the UPRAAM

The majority, if not all, of these principles can be identified in the EU GDPR and/or the draft modernised CoE Convention 108. The principles assume the existence of a supervisory authority, but not necessarily a single supervisory authority.

1. **Universality Principle**: Data protection rights should apply to all data subjects, regardless of their nationality or residence.

2. **Collection Limitation Principle**: Collection of personal data should be limited, lawful and by fair means; and made on the basis of unambiguous, demonstrable and continuing consent, or demonstrable knowledge (where consent is not required). Separate consent should be required for each item requiring consent (unbundling).

3. **Purpose Limitation Principle**: Personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, unless for legitimate and proportionate purposes permitted by law.

4. **Data Minimisation Principle**: Personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

5. **Accuracy Principle**: Personal data should be accurate and, where necessary, kept up to date; reasonable measures should be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed, are erased or rectified in reasonable time.

6. **Storage Limitation Principle**: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed, unless it is to be processed solely for legitimate and proportionate purposes specified by law.

7. **Sensitive Data Principle**: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation, criminal convictions and offences or related security measures should not be processed without the data subject’s explicit consent, unless for legitimate and proportionate purposes specified by law.

8. **Protection of Minors Principle**: Special protection, or prohibition of personal data collection, should be considered in circumstances where minors might be at risk of providing personal data without adequate safeguards, for instance, in order to access or use information society services.

9. **Transparency Principle**: A data subject from whom personal data is collected should be provided with, at the time of collection (or if the personal data have not been obtained from the data subject, within a reasonable period) sufficient information to exercise their rights e.g. the identity and the contact details of the controller and/or their representative; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the categories of personal data concerned; any recipients or categories of recipients of the personal data; details of any transfer to a recipient in a third country or international organisation. He or she should be able to obtain from the controller confirmation as to whether or not their personal data are being processed and to access the personal data and such information about the processing as is necessary to exercise their rights.

10. **Rectification Principle**: A data subject should have the right to obtain from a data controller without undue delay the rectification of inaccurate personal data concerning him/her.

11. **Erasure Principle**: Subject to limited public policy exceptions, a data subject should be able to require a data controller to erase personal data: which are no longer required for the purposes for which they were collected; for which consent is required and has been withdrawn; the processing of which the data subject may object to in law; or which are otherwise processed unfairly or unlawfully.
12. **Restriction principle**: A data subject should have the right to obtain from the controller restriction of processing where the personal data is the subject of dispute between data subject and data controller, or where the data would normally be erased but it is in the interest of the data subject, that the data be retained, with limited access.

13. **Data Portability Principle**: The data subject should have the right to receive their personal data, which he/she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

14. **Automated Processing Principle**: The data subject should have the right to know when they are subject to a decision based solely on automated processing, including profiling, which produces legal or significant effects concerning him or her.

15. **Security Principle**: Personal data should be processed securely with protection by appropriate contextual technical or organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

16. **Data Breach Principle**: Data controllers should notify a personal data breach to the competent supervisory authority without undue delay. Where the personal data breach is likely to result in a high risk to the rights of a data subject, the controller should notify the personal data breach to the data subject without undue delay.

17. **Accountability Principle**: Both data controllers and data processors should be demonstrably accountable for complying with measures which give effect to these principles. Data controllers should be able to demonstrate that they have given appropriate consideration to the contextual risks to the rights of data subjects prior to processing (privacy impact assessment); that they have consulted with their supervisory authority where that consideration suggests a high risk (prior consultation); and that they have taken steps to build into their processing practices appropriate contextual technical and organisational measures to protect the rights of data subjects (privacy by design/default).

18. **Data Transfer Principle**: A data controller or processor may transfer personal data to a third country or an international organisation, if it ensures an adequate level of protection. Where a third country or an international organisation does not have an adequate level of protection, a data controller or processor may transfer personal data to them only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; where the data subject has given explicit unambiguous and demonstrable consent to the proposed transfer; or where there are legitimate and proportionate purposes specified by law.

Insofar as these principles are reflected within the current and future EU data privacy framework, they form the basis for determining the following detailed obligations for the UPRAAM.
6.2 List of detailed obligations

6.2.1 Obligations premised on the EU Framework

This Subsection identifies the set of legal obligations in terms of privacy and data protection defined by the EU directives, Directive 95/46/EC (Data protection Directive) and Directive 2002/58/EC (ePrivacy Directive).

To provide a fully compliant methodology with EU law scenarios, this analysis also takes into account relevant Opinions of Article 29 Working Party (hereinafter, “Art.29 WP”) and any new provisions introduced by the General Data Protection Regulation (GDPR).

6.2.1.1 End-user information

This set of obligations includes all the information that must be given to data subjects before the data collection in terms of processing, consent, rights and minors of age’s means of protection.

A. Information to the user

The data subject must receive accurate and full information about the processing. Information may be provided through a system of layered notices, push messages and combined with meaningful icons.

Detailed description:

Apps, websites and IoT deployments should provide the user with information on at least the following elements:

a) the identity of the controller and of his representative, if any;

b) the purposes of the processing for which the data are intended;

c) any further information such as:

- the recipients or categories of recipients of the data;
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data concerning him.

This information must be provided to the data subject even if the data have not been obtained from the data subject. In this case, the controller or his representative must provide it at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Legal basis:

Data Protection Directive (95/46/EC): Articles 10 and 11.

B. Prior consent

Apps, websites, IoT deployments must ask for consent before they start to retrieve or place information on the device, i.e., before installation of the app, cookie, tracker etc. Such consent has to be freely given, specific and informed (see above, Information to the user).

Detailed description:

Consent should be granular for each type of data accessed; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card
and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics.

Legal basis:

C. Prior consent

Apps, websites, IoT deployments must enable users to exercise their rights of access informing them about the existence of these mechanisms and supporting efficient access by the data subjects to their personal data.

Detailed description:
The exercise of users’ rights must be easy and without formalities. Having regard to the right of access, each user, acting as a data subject, has the right to obtain from the controller, without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed and information as to the purposes of the processing, the categories of data concerned, and the recipients to whom the data are disclosed.

Legal basis:

D. User’s right to have his/her personal data rectified, blocked or erased

Apps, websites, IoT deployments must enable users to exercise their rights of rectification, erasure and blocking and inform them about the existence of these mechanisms.

Detailed description:
The exercise of users’ rights must be easy and without formalities. Having regard to the right to have his personal data rectified or erased, each user, acting as a data subject, has the right to obtain from the controller the modification of data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed. Data controllers must also notify to third parties to whom the data have been disclosed any rectification, erasure or blocking operation – unless it is impossible or requires a disproportionate effort.

Legal basis:
Data Protection Directive (95/46/EC): Articles 6(d), 12(b) and 12(c).

E. User’s right to object

Apps, websites, IoT deployments must enable users to exercise their right to object to data processing and inform them about the existence of this mechanism.

Detailed description:
The data subject has right to object:
- at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation, at least when his data are processed by a public authority or by a data controller relying on its legitimate interest;
- on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Legal basis:

F. User’s right to be forgotten (online environment)

Apps, websites, IoT deployments must enable users to exercise their right to be forgotten when the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed. Especially, it refers to the right to remove from the web the results obtained from searches made on the basis of his name, unless a greater interest to transparency prevails.

Detailed description:
In the online environment, the right to erasure should be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers who are processing such data to erase any links to, or copies or replications of that personal data. This right does not require deletion of the link from the indexes of the search engine altogether: therefore, the original information will always be accessible using other search terms, or by direct access to the source.

Legal basis:
GDPR: Article 17.

6.2.1.2 Data collection

This set of obligations refers to the processing operations that the data controller can carry out after data collection.

A. Purpose limitation

Apps, websites, IoT deployments must provide well-defined and comprehensible purposes of the data processing in advance to installation of the app, cookies or any other tracker.

Detailed description:
Purposes cannot be changed without renewed consent. The app, website, IoT tool should provide comprehensive information, also for users without legal or technical knowledge, so as to clarify if the data will be used for third party purposes, such as advertising or analytics.

Legal basis:
- Data Protection Directive (95/46/EC): Articles 2(b) and 6(1) b).

B. Data control

Whenever apps, websites, IoT deployments process data, it must be clear who or what is the entity governing the process, i.e., who is the data controller. The data controller is legally responsible for any processing operation (collection, recording, organization, storage, adaptation or alteration,
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction). The data controller remains responsible even if he designates a data processor acting on his behalf.

Detailed description:

The data ‘controller’ is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The data ‘processor’ is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller and acting only on instructions from the controller.

Legal basis:
- Data Protection Directive (95/46/EC): Article 2(b), (d) and (e), Article 10(a), Article 16 and Article 17(3).

C. Data minimization

Apps, websites, IoT deployments should respect the principle of data minimisation and only collect those data that are strictly necessary to perform the desired functionality.

Detailed description:

Collected data must be adequate, relevant and not excessive in relation to the purposes for which they are processed, in order to prevent unnecessary and potentially unlawful data processing.

Legal basis:
- Data Protection Directive (95/46/EC): Article 6(1) c).

D. Data profiling

Apps, websites, IoT deployments must not profile users without their specific and explicit consent for purposes of behavioural advertising.

Detailed description:

Evaluate personal aspects relating to a natural person, in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements is forbidden without a user specific and explicit consent. In this sense, the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information.

Legal basis:
- GDPR: Article 20(3).

E. Geolocation

Apps, websites and IoT deployments must not geographically locate users without their prior and specific consent.

Detailed description:
The app, website or IoT tool should also activate an icon every time the geolocation is on.

Legal basis:

**F. Direct marketing**

Apps, websites and IoT deployments must not target users and subscribers for direct marketing purposes, through electronic means without their prior and specific consent.

Detailed description:

The app, website or IoT tool should ask a specific consent before sending such messages. Moreover, there must be an “opt-out” option to ensure the consent withdrawal, providing users with a valid mean (e-mail address, form etc.) through which he can send the request. The identity of the sender on whose behalf the communication is made must be clearly indicated to recipients of the commercial message.

Legal basis:

**G. Data of Minors**

Apps, websites, and IoT deployments should pay attention to the age limit defining children or minors in national legislation, choose the most restrictive data processing approach in full respect of the principles of data minimization and purpose limitation, refrain from processing children’s data for behavioural advertising purposes, either directly or indirectly and refrain from collecting data through the children about their relatives and/or friends.

Detailed description:

Apps, websites and IoT deployments should provide an automatic age control mechanism in order to reduce the risk of collect accidentally children’s data and for the purpose of protecting their data and avoiding unlawful consent.

The GDPR considers the data processing of a child below the age of 16 years (or if provided for by Member State law a lower age which shall not be below 13 years) lawful only if the consent of the minor is given or authorised by the holder of parental responsibility over the child. The burden of verifying that the consent is given or authorized by a parent is up to the controller.

Legal basis:
- GDPR: Article 8.

6.2.1.3 Data management

This set of obligations concerns the retention and the disclosure to third parties of personal data after having collecting them.

**A. Data retention and erasure**

Apps, websites, IoT deployments should define a reasonable retention period for data collected and predefine a period of inactivity after which the account will be treated as expired.
Detailed description:
Data must be erased upon expiration of the retention period, save the obligation to keep them longer in accordance with law.

Legal basis:

B. Data disclosure to third parties

Apps, websites, IoT deployments should inform users about recipients or categories of recipients to whom the data are disclosed.

Detailed description:
Users must be informed (see Information to the user) about the eventuality of data disclosure when receiving the information, identifying to whom personal data is disclosed. These third party recipients must be informed that they should only use the data for the purpose(s) for which they are provided.

Legal basis:

6.2.1.4 Data processing

This set of obligations considers any operation or set of operations which is performed upon personal data, whether or not by automatic means (collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, destruction).

A. Special categories of data

Each data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life must be processed only under certain circumstances.

Detailed description:
Normally, the process of special categories of data is forbidden, but it is possible if the data subject has given his/her explicit consent or if processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law; or processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Moreover, it is possible when purposes concern preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by
national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority.

Legal basis:

**B. Traffic data**

The technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user is allowed.

Detailed description:

Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

For the purpose of marketing electronic communication services or for the provision of value added services, traffic data can be processed only if the subscriber or user to whom the data relate has given his/her consent (which can be withdrawn at any time).

Legal basis:

**C. Security of the processing**

The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Detailed description:

Technical and organizational measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. In this sense, the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures.

The same measures to safeguard security of services are provided in case of electronic communications service. In particular, the controller has to inform the user and the National Supervisory Authority about the risks or the occurred breach of the security and about any possible remedies.

An example of such measures is the use of an authentication and authorization system. Persons in charge of the processing shall be allowed to process personal data by electronic means only if they are provided with authentication credentials with which complete the authentication procedure. These credentials must be composed by a personal ID code and a secret password.
with at least eight characters (if this is not allowed, the password could consist of the maximum permitted number of characters). It shall be modified at least every six months. Alternatively, these credentials shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing or in a biometric feature (possibly, in both cases, associated with either an ID code or a password).

Clearly, each person in charge of the processing will have a different authorization profile, relating either to a specific processing operation or to a set of processing operations.

Other examples of security measures are the periodical back-up procedure, which aim is to ensure the continuity of the system and prevent the loss of data or the data encryption, that must be applied to all personal and authentication data, in order to make users’ data and credentials encoded in non-readable format even if the stability of the system is compromised. Authentication credentials shall be de-activated if the person in charge of the processing is disqualified from accessing personal data.

Legal basis:

D. Notification and prior checking

The controller must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

In case of processing that presents specific risks to the rights and freedoms of data subjects these processing operations are examined prior to the start thereof by the supervisory authority following receipt of a notification from the controller.

Detailed description:

In case of a wholly or partly automatic processing operation, the controller must notify the supervisory authority:
(a) the name and address of the controller and of his representative, if any;
(b) the purpose or purposes of the ‘processing; (c) a description of the category or categories of data subject and of the data or categories of data relating to them; (d) the recipients or categories of recipient to whom the data might be disclosed; (e) proposed transfers of data to third countries; (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.

Legal basis:
- Data Protection Directive (95/46/EC): Articles 18, 19 and 20.

E. Cloud services

Cloud computing services are offered by cloud providers by means of standard and unmodifiable contracts, which may make difficult for clients, which are data controllers under EU law, to ensure the compliance with data protection rules.

Detailed description:

The controllership of data processing belongs to the client, whereas the cloud service provider is usually the data processor. So, the client is responsible and subject to all the legal duties provided for by Directive 95/46/EC. However, by using a data processing agreement, the controller can leave to the processor a certain level of autonomy regarding technical and organizational measures needed to achieve purposes of the data controller. In parallel, the cloud...
service provider must ensure that personal data are processed in a secure manner, pursuant to Article 17 (3) Directive 95/46/EC. In order for the client to verify whether such a level of security and compliance with data protection law is guaranteed by the provider, it proves to be very useful to check the Privacy Level Agreements (PLAs) offered by the latter; these PLAs may also include provisions concerning the exercise of data subject’s rights.

With reference to the level of services provided by the cloud service provider, Service Level Agreements (SLAs) identify not only the services but also the objectives that the cloud provider offers to the client in terms of security (uptime, reliability, authentication and authorization, breaches reporting etc.) and data management (retention, erasure etc.).

Following Article 4 of Directive 95/46/EC, if the data controller (client) is established in the EEA, the applicable law is the one of the Member State where it is established; if it is established in different countries, the applicable law is that of each of the Member States in which the processing of personal data occurs.

In case of a client (controller) established outside the EEA, if the cloud infrastructures are located in the EEA, then the processing is governed by the law of the Member State where the infrastructures (i.e. equipments) are.

The cloud service provider may avail itself of sub-contractors so as to carry out part of the data processing and the former must ensure that its sub-contractors are contractually bound to him respecting the same obligations and standards he has agreed to with the data controller – for example, he can use model contractual clauses, especially if these subcontractors are located outside the EU.

Legal basis:

Data Protection Directive (95/46/EC): Articles 4 and 17(3).
6.3 Synthetic matrix

Following the detailed breakdown of legal obligations in the previous subsection, it is possible to divide the methodological approach into two different analytical perspectives:

- **The end-user perspective:** which considers his/her potential level of privacy risks in terms of data protection offered by a data controller from whom the data subject is receiving a service (IoT, smartphone app, website);

- **The SMEs perspective:** in which the enterprise personifies the data controller and therefore it has to evaluate its level of compliance in terms of data processing.

The table that follows synthesizes the obligations, prior to the splitting of these two perspectives.

<table>
<thead>
<tr>
<th><strong>End-user information awareness</strong></th>
<th>Information to be given to the user:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• the identity of the controller and of his representative, if any;</td>
</tr>
<tr>
<td></td>
<td>• the purposes of the processing for which the data are intended;</td>
</tr>
<tr>
<td></td>
<td>• any further information such as:</td>
</tr>
<tr>
<td></td>
<td>- the recipients or categories of recipients of the data</td>
</tr>
<tr>
<td></td>
<td>- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,</td>
</tr>
<tr>
<td></td>
<td>- the existence of the right of access to and the right to rectify the data concerning him</td>
</tr>
</tbody>
</table>

Prior consent for:

- marketing purposes;
- disclosure to third parties;
- geolocation;
- profiling (it may include data such as contacts, browsing history, duration of navigation, frequency of certain queries etc. and be performed through cookies);

or for special categories of data, revealing\(^3\):

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;

---

\(^3\) These are not PF obligations. These are obligations for controllers. Starting from them we identify the questions for the UPRAAM, so in this case the question could be “if the controller has collected your data revealing racial origin, political opinions etc., has he asked for your consent before the processing?”
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

- trade-union membership;
- data concerning health;
- data concerning sex life;

or for processing about:
- contacts;
- calendar;
- social networks credentials;
- biometrics.

Right of access of the data subject to his/her personal data without excessive delay or expense, confirmation as to whether or not data relating to him/her are being processed.

Right of the data subject to have his/her personal data rectified, blocked or erased.

Right of the data subject to object at any time, on compelling legitimate grounds relating to his/her particular situation, to the processing of data relating to him.

Right to be forgotten - the right for the user to remove from the web the results obtained from searches made on the basis of his/her name, unless a greater public interest for transparency prevails.

Full user control over his/her personal data.

| Data collection | Purposes limitation (purpose(s) cannot be changed without renewed consent).
| Data control (data controller is legally responsible for any processing operation even if he designates a data processor acting on his behalf). |
| Data minimization (anonymization and pseudonymization are preferred and, in general, the only data that must be collected are those which are strictly necessary to perform the desired functionality). |
| Profiling (evaluation of personal aspects relating to the data subject, analysing and predicting aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements is forbidden without a user specific and explicit consent). |
| Geolocation must be carried out with the data subject’s prior and specific consent, activating an icon every time geolocation is turned on. |
| Direct marketing operations must be preceded by a specific consent. Moreover, there must be an “opt-out” option to ensure the ability to withdraw consent. |

| Data management | Retention and erasure (the data controller must define a reasonable retention period for data collected and predefine a period of inactivity after which the account will be treated as expired). |
Disclosure to third parties is not just a part of the information to be given to the user, but also concerns those third party recipients, who must be informed that they should only use the data for the purpose(s) for which it was provided.

### Data processing

Special categories of data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life) must be processed only under certain circumstances.

Traffic data related to subscribers and users that are processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication.

Security of the processing must be ensured by the data controller with appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Notification and prior checking (notification to the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes; in case of processing that presents specific risks to the rights and freedoms of data subjects these processing operations are examined prior to the start thereof by the supervisory authority following receipt of a notification from the controller).

Cloud services implicate that the controllership of data processing belongs to the client, whereas the cloud service provider is usually the data processor. So, the client is responsible and subject to all the legal duties provided for by Directive 95/46/EC. However, by using a data processing agreement, the controller can leave to the processor a certain level of autonomy regarding technical and organizational measures needed to achieve purposes of the data controller. In parallel, the cloud service provider must ensure that personal data are processed in a secure manner by signing a Privacy Level Agreements (PLAs).

### 6.3.1 The Perspective of an End-User

Working from the previous categorization, it is now possible to gather the different obligations into further list taking an end-user perspective, that is, considering those kinds of obligations that have an effective impact on an end user’s privacy risk level evaluation.

Those obligations can be divided into three different categories:

1. **End-user awareness**, which includes all the information that must be given to users before data collection, including his/her prior consent, where provided for by law.
2. End-users’ rights, the data subject not only has the right to be informed, but also to have access to his/her personal data, and, if appropriate, to see his/her data rectified, blocked or erased, or to object to the processing of his/her personal data, these rights guaranteeing his/her effective control over the data.

3. The processing operations, which refer to the definition of purposes and the operations of minimizations. Protection of minors and data transfer to third parties fall within this perspective. The table on the following page outlines the obligations from the end-user’s perspective.

<table>
<thead>
<tr>
<th>End user information awareness</th>
<th>Information to be given to the user</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prior consent for:</td>
</tr>
<tr>
<td></td>
<td>• marketing purposes;</td>
</tr>
<tr>
<td></td>
<td>• disclosure to third parties;</td>
</tr>
<tr>
<td></td>
<td>• geolocation;</td>
</tr>
<tr>
<td></td>
<td>• profiling (it may include data such as contacts, browsing history, duration of navigation, frequency of certain queries etc. and be performed through cookies);</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or for special categories of data, revealing 308:</td>
</tr>
<tr>
<td></td>
<td>• racial or ethnic origin;</td>
</tr>
<tr>
<td></td>
<td>• political opinions;</td>
</tr>
<tr>
<td></td>
<td>• religious or philosophical beliefs;</td>
</tr>
<tr>
<td></td>
<td>• trade-union membership;</td>
</tr>
<tr>
<td></td>
<td>• data concerning health;</td>
</tr>
<tr>
<td></td>
<td>• data concerning sex life;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or for processing about:</td>
</tr>
<tr>
<td></td>
<td>• contacts;</td>
</tr>
<tr>
<td></td>
<td>• calendar;</td>
</tr>
<tr>
<td></td>
<td>• social networks credentials;</td>
</tr>
<tr>
<td></td>
<td>• biometrics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>End-user’s right</th>
<th>Right of access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Right to have his/her personal data rectified, blocked or erased</td>
</tr>
<tr>
<td></td>
<td>Right to object</td>
</tr>
<tr>
<td></td>
<td>Right to be forgotten</td>
</tr>
</tbody>
</table>

308 In fact there is a prior consent requirement. The prior consent follows the information to be given to the data subject and both of them are part of the end-user information awareness.
Full user’s control on his/her personal data

<table>
<thead>
<tr>
<th>Data collection</th>
<th>Purpose limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data minimization</td>
</tr>
<tr>
<td></td>
<td>Transfer to third countries</td>
</tr>
<tr>
<td></td>
<td>Avoidance of data collection of minors</td>
</tr>
</tbody>
</table>

6.3.2 The Perspective of an SME

In terms of data protection, the enterprise must ensure that all the personal data obtained about data subjects are processed lawfully. In this sense, compared to the list of relevant obligations identified from the end-user perspective, the list provided for an SME evaluation has to consider further aspects, concerning data management and all the operations carried out since the moment of data collection, including those technical aspects, such as the use of anonymization/pseudonymization techniques, or adoption of different security measures, that the end-user may not be aware of.

Maintaining the categorization previously identified, it is possible to readapt this approach so as to examine the enterprise’s internal adjustment required to be compliant with the obligations provided for by law:

- **End-user awareness**, which refers to all the information that must be given to users before the data collection, as well as information that is ancillary, but can further clarify the processing operations to the user. It also analyses the source of the collection (the data subject themselves, or other sources), including aspects relating to prior consent, if provided for by law, and focusing on the mechanism of consent withdrawal and its consequences.

- **End-user rights**, in order to understand if the data controller is providing the user with appropriate means to allow him/her to exercise his/her rights.

- **The data management**, which refers to collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure and destruction.
  - This all-encompassing section permits to identify which kind of personal data are processed and if the data controller follows the data minimization principle, eventually processing the data for additional purposes that are incompatible with the original aim of the processing. Moreover, it refers to the presence (or absence) of a data processor acting on behalf of the controller and all the security measures provided since the collection to the storage (and erasure), especially in case of data breaches, also considering the presence of a Data Protection Officer (DPO) and the measures adopted in order to avoid minors’ data collection.
  - The relationship with the data protection authority must be examined too, considering the mechanisms of prior checking and notification provided for by law in certain cases of data processing.

So as to complete the analysis, it is useful to know if there is a data disclosure to third parties or transfer outside the EEA or if the data controller uses cloud services processing data in cloud systems and where are located the servers.
Table 5: Obligations: The perspective of an SME

<table>
<thead>
<tr>
<th>End-user information awareness</th>
<th>Information to be given to the user</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Additional information provided with the notice</td>
</tr>
<tr>
<td></td>
<td>Sources of the collection</td>
</tr>
<tr>
<td></td>
<td>Prior consent for:</td>
</tr>
<tr>
<td></td>
<td>• marketing purposes;</td>
</tr>
<tr>
<td></td>
<td>• disclosure to third parties;</td>
</tr>
<tr>
<td></td>
<td>• geolocation;</td>
</tr>
<tr>
<td></td>
<td>• profiling (it may include data such as contacts, browsing history, duration of navigation, frequency of certain queries etc. and be performed through cookies);</td>
</tr>
<tr>
<td></td>
<td>or for special categories of data, revealing:</td>
</tr>
<tr>
<td></td>
<td>• racial or ethnic origin;</td>
</tr>
<tr>
<td></td>
<td>• political opinions;</td>
</tr>
<tr>
<td></td>
<td>• religious or philosophical beliefs;</td>
</tr>
<tr>
<td></td>
<td>• trade-union membership;</td>
</tr>
<tr>
<td></td>
<td>• data concerning health;</td>
</tr>
<tr>
<td></td>
<td>• data concerning sex life;</td>
</tr>
<tr>
<td></td>
<td>or for processing about:</td>
</tr>
<tr>
<td></td>
<td>• contacts;</td>
</tr>
<tr>
<td></td>
<td>• calendar;</td>
</tr>
<tr>
<td></td>
<td>• social networks credentials;</td>
</tr>
<tr>
<td></td>
<td>• biometrics.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>End-user’s right</th>
<th>Right of access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Right to have his/her personal data rectified, blocked or erased</td>
</tr>
<tr>
<td></td>
<td>Right to object</td>
</tr>
<tr>
<td></td>
<td>Right to be forgotten</td>
</tr>
<tr>
<td></td>
<td>Full user’s control on his/her personal data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data management</th>
<th>Personal data processing (kind of data processed)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Purposes limitation and compatibility of new purposes with the original aim of the processing</td>
</tr>
<tr>
<td></td>
<td>Data minimization and adoption of anonymization or pseudonymization techniques</td>
</tr>
<tr>
<td></td>
<td>Data control (presence of a data processor acting on behalf of the controller)</td>
</tr>
<tr>
<td>Security measures (alteration, loss, breaches, back-ups, authentication and authorization systems, DPOs)</td>
<td></td>
</tr>
<tr>
<td>Avoidance of minors’ data collection</td>
<td></td>
</tr>
<tr>
<td>Prior checking and notification</td>
<td></td>
</tr>
<tr>
<td>Data disclosure</td>
<td></td>
</tr>
<tr>
<td>Transfer to third countries</td>
<td></td>
</tr>
<tr>
<td>Cloud services</td>
<td></td>
</tr>
</tbody>
</table>
7. Summary and Conclusion

This report has analysed a range of existing legal frameworks with a focus on European and international norms related to personal data protection, privacy and data ownership. It has identified and categorised the:

- personal data protection and privacy obligations and norms that have been developed in key national and supra-national jurisdictions, and which play a primary role in influencing international governmental and commercial practices;
- obligations and norms which have developed and promoted by means of international Guidelines, Agreements and Conventions.

It has then provided a set of clear and concise legal requirements via a synthesis of the legal risks that the Privacy Flag project will address via its UPRAAM.

The survey of international privacy and data protection standards (Section 3.6) concluded that there are a reasonably coherent and stable set of core principles that have been developed since the 1970s, e.g. the OECD Guidelines and CoE Convention 108, and which are widely accepted by States, even if implementation of those principles may vary significantly in practice. If those standards can be considered the first generation of data privacy norms, and the EU DPD the second generation, then it appears that a third generation e.g. the modernised Convention 108 and the EU GDPR has now appeared, which seek to address the emerging environmental contexts created by technological advances in data processing and the impact of networks and globalisation upon data transfers. The third generation of norms largely retain the core principles from the first and second generations, and have incorporated into that core set of principles concepts that were once outliers, e.g. the need for an independent national supervisory body with investigation and enforcement powers. The EU has been, and continues to be, a prime mover in this ‘third generation’ thinking.

Review of the development of European principles and norms (section 4.5) concluded that the goal of harmonising data privacy laws across the EU has been successful to the extent that the EU has been able to agree the new GDPR in 2016, but EU data protection ecosystem remained complex, with variations in terms of national legislation and case law, national regulatory oversight, and administrative practices. The directly applicable GDPR will continue, and probably hasten, the slow convergence of public and private sector practice across the EU.

The EU data privacy framework being premised on a human rights foundation, reinforced by the incorporation of data privacy rights in the EU Charter of Fundamental Rights and the prior and ongoing jurisprudence of the ECHR, differentiates it from some national and regional data privacy regimes which, in relation to the private sector at least, have tended to be predicated on pragmatic consumer protection/commercial trust (e.g. the common law jurisdictions) and facilitating transborder data transfers (the APEC framework).

Criticisms of the EU framework include that it is over-bureaucratic, and tends to focus upon meeting administrative formalities rather than actual privacy outcomes. This may cause organisations to develop management systems that are compliance-focused and inward-looking, rather than
Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426

proactive, predictive and reflexive. The increased importance assigned in the GDPR to the principle of accountability, the proposed reduction in formalism, and the incorporation of mechanisms such as privacy by design and privacy impact assessments appear to be a response to such criticism.

The survey of international frameworks and national laws concluded (Section 5.6) that the international data privacy landscape has changed rapidly over the last decade, but the principles and norms in the OECD Guidelines and CoE Convention widely underpin national data privacy frameworks and regional agreements/guidelines, even where the protection of human rights is not a primary driver. Even where countries have weak or no data privacy frameworks, the influence of those principles and norms can still be discerned in either legislative/regulatory terminology, or in sectoral practices.

The Art.25 ‘adequacy’ process in the EU DPD has also had a major influence on non-EEA states, encouraging them to adopt norms and practices that aim, if not to precisely mirror the EU legislation, then at least to achieve the same purposive ends. This means that in practical terms, an organisation meeting the requirements of the EU DPD will currently ensure a high level of compliance with the majority, if not all, of the current data protection regimes world-wide.

Developments in other jurisdictions have had demonstrable effects in improving both data privacy and data security. The common law jurisdictions have led the way in developing practical solutions for embedding data privacy in public and private sector work flows (e.g. PIAs and privacy by design), and have had some success in utilising regulatory tools such as self-regulation, co-regulation, market forces through non-traditional means, such as sectoral regulators (e.g. the FTC) and data breach notification laws. The EU GDPR reflects the success of these mechanisms by incorporating them into the future EU data privacy framework.

Section 6 provides a set of Third Generation ‘core’ principles (6.1.1), which while not yet of universal application, even within the EU data privacy framework, are suggested as key principles to be adopted within the UPRAAM. It then provides an assessment of the obligations that would arise in the context of the environments in which the Privacy Flag project intends to operate.
8. List of references

All web links accurate as of 20 May 2016.

8.1 Publications of International Organisations


---. (1973). Resolution 73(22) on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector, available from the COE Documents data base at [https://wcd.coe.int/](https://wcd.coe.int/)


---. (1999). Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede (15 June 1999), available at: [http://www.coe.int/t/dghl/standardsetting/dataprotection/Amendments%20to%20the%20Convention%20108.asp](http://www.coe.int/t/dghl/standardsetting/dataprotection/Amendments%20to%20the%20Convention%20108.asp)


Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426


--. Art.29 Working Party, Opinion 04/2012 on Cookie Consent Exemption WP 194, 00879/12/EN.

--. Art.29 Working Party, Opinion 02/2013 on apps on smart devices, WP 202, 00461/13/EN.


--. Art.29 Working Party (2016). Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 16/EN.


Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployment (Privacy Flag) GRANT AGREEMENT NO.653426


8.2 State Publications


8.3 Academic, Corporate and NGO publications


Privacy International (undated) *Submissions to the UN*. https://www.privacyinternational.org/reports/submissions-to-the-un


