International
Comparative
Legal Guides

Data Protection 2021

A practical cross-border insight into data protection law

Eighth Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Data Protection 2021

Eighth Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

ICLG.com

Privacy By Design as a Fundamental Requirement for the Processing of Personal Data

FABIAN PRIVACY LEGAL GmbH

Daniela Fábián Masoch

Privacy by design ("PbD") is a fundamental requirement for privacy-compliant processing of personal data and is, in principle, a well-known approach. Nevertheless, PbD is often not consistently implemented, in some cases leading to significant consequences and costs for organisations. This article describes the concept of PbD and its practical implementation under the application of the European Union ("EU") General Data Protection Regulation (EU) 2016/679 of 27 April 2016 ("GDPR").

1 Introduction

The ongoing development of new and complex technologies such as artificial intelligence ("AI"), blockchain, or the Internet of Things ("IoT") and their increasing use, as well as ongoing digitisation and centralisation of data management, are leading to increasingly sophisticated ways of automating the processing of enormous amounts of data, facilitating data flows and availability, profiling consumers, customers, patients, or job applicants, and making automated decisions.

To reap the benefits of these technologies, digitisation, and new business models in connection with the processing of personal data, those who develop or deploy them must consider and implement applicable data protection principles and requirements through appropriate and adequate technical and organisational measures from the outset, already at the design stage, and continuously monitor, adjust and update them throughout the lifecycle of the system, product, or process.

With this PbD approach, a company can ensure compliance with legal requirements, meet the expectations of individuals and stakeholders, build trust, make strategic and operational decisions with foresight and efficiently implement business processes. This can include, for example, storing data on servers in the EU or Switzerland instead of in the USA or purchasing software with integrated data protection principles.

PbD has become a critical factor in building and maintaining trust, competitiveness and success in the marketplace.

2 The Concept of PbD

The concept of PbD is a fundamental requirement for the effective implementation of data protection. In essence, PbD requires that controllers consider data protection principles and requirements both at the design stage of systems, processes, products or services that involve the processing of personal data, and throughout the lifecycle of personal data, and that they provide for appropriate technical and organisational measures ("TOMs") to implement data protection requirements and protect the rights of data subjects. Controllers must be proactive and anticipate potential privacy intrusions before they occur.

One of the fundamental elements of PbD is "privacy by default". This concept requires that the controller implements appropriate TOMs to ensure that, by default, only personal data that is necessary to fulfil the specific purpose is processed. PbD must be implemented in terms of the amount of data collected, the scope of its processing, the duration of its storage, its security, and its accessibility.

While the concept of PbD has long existed as good practice, it was introduced as a legal obligation for controllers in Art. 25 GDPR, with significant fines for non-compliance. In introducing the PbD concept, the legislator primarily wanted to emphasise that it is not enough to set standards, and that the controller must also *implement* these standards in an effective and verifiable manner. Other laws have also adopted the concept of PbD, most recently the new Swiss Federal Act on Data Protection ("nFADP"), which is expected to come into force in 2022. However, unlike the GDPR, under the nFADP a breach of the new PbD obligation will have no direct consequences.

However, neither the GDPR nor the nFADP specify how the controller should implement PbD in practice.

So far, the introduction of processes and the designation of responsibilities for the systematic and timely assessment of the planned data processing, the technologies and systems used for this purpose and the data protection risks for the data subjects have proven effective. This risk assessment aims to identify the technical and organisational measures required to effectively integrate data protection principles and requirements into the design of the respective products, systems or processes and to protect the privacy of the data subjects. Risks to data subjects include, for example, excessive collection and disclosure of personal data, processing of data for purposes other than the original purpose, unlawful processing, as well as loss, destruction or alteration of data.

Such a risk assessment, coupled with a compliance assessment, is required for any processing of personal data, including, for example, the implementation of a Customer Relation Management ("CRM") or HR data management system or the outsourcing of data processing, regardless of the technology used or the sensitivity of the data. While similar, this risk and compliance assessment is not a data protection impact assessment ("DPIA") as required under Art. 35 GDPR.

A controller must conduct a DPIA only if the processing is likely to present a high risk to data subjects' rights and freedoms. A DPIA is a broader assessment that goes beyond a compliance assessment by evaluating the residual risks to data subjects, taking into account the TOMs embedded in the design of the product, system or process. If the residual risk is still considered high, the controller must take further measures to mitigate the risk. If this is not possible, the controller must consult the data protection authority or refrain from processing. A DPIA will be regularly required for digital health solutions

where health-related data or other special categories of data are processed. A DPIA will also be regularly required for the use of innovative or combined technologies and extensive profiling.

3 Implementing PbD In Practice

3.1 Technical and organisational measures

The controller must implement TOMs both at the time of determining the means of processing and during the processing itself. The TOMs must be adequate and appropriate to:

- effectively implement data protection principles, such as data minimisation, lawfulness, transparency, confidentiality, purpose limitation, data integrity, storage duration, security, as well as the requirements concerning commissioned data processing and cross-border data transfers;
- integrate the necessary safeguards into the processing to meet the requirements of the GDPR; and
- protect the rights of data subjects.

A measure is adequate if it considers state of the art, the cost of implementation, the nature, scope, context and purposes of the processing, and the risks of varying likelihood and severity to natural persons' rights and freedoms.

Technical measures may include, for example:

- robust encryption methods for systems and data;
- pseudonymisation or aggregation of the data;
- access authorisations and restrictions;
- user authentication;
- firewalls; and
- automated deletion concepts.

Organisational measures may include, for example:

- the assignment of responsibilities for the effective implementation of data protection requirements;
- the implementation of enforceable policies and procedures for handling and documenting data privacy violations and requests for information from data subjects, risk management, third-party vendor management, data transfer management, and the documentation of processing activities;
- the implementation of training and controls; and
- the establishment of processes to ensure data protection rights, such as revoking consent or requesting erasure of the data.

3.2 Data Protection Management System (Fig.1)

One effective way to implement PbD in practice is to build a data management and risk assessment programme with responsibilities and a process to systematically identify, evaluate, address and mitigate potential privacy and security risks associated with the collection and processing of personal data. A Data Protection Management System should include the following elements:

- a documented ***commitment*** by the company's management to establish and enforce high standards of data protection for the company, to integrate data protection into the corporate culture and embed the data protection principles in the design and implementation of corporate policies, data protection management systems, business practices, services and products;
- the appointment of a data protection officer or advisor and the allocation of ***responsibilities*** at all levels of the organisation, including business units and functions, for the effective implementation of data protection requirements;
- the establishment of a data protection ***framework*** with enforceable data protection policies and guidelines that attach appropriate importance to data protection and regulate the collection, processing, transfer, storage and deletion of data, as well as mechanisms to monitor implementation and compliance with standards and rules;
- the application of appropriate ***processes*** to ensure that data protection principles and requirements are adequately taken into account and integrated into data processing procedures and that the PbD principle is thus lived;
- the introduction of ***records of processing activities*** ("RoPA");
- ***risk management*** with risk assessments, compliance checks and, where appropriate, data protection impact assessments;
- ***third-party management*** and ***data transfer governance***;
- regular and documented ***awareness*** campaigns and conducting employee ***training***; and
- regular and documented ***monitoring and controls*** through self-assessments and audits to verify the effective implementation of the data protection management programme and compliance with legal requirements and internal policies and directives.

3.3 Data protection considerations and design strategies

Applicable laws

The controller must clarify the applicable laws and regulations. In particular, organisations outside the EU must determine whether the GDPR applies to them and their activities. The controller should also check whether industry-specific codes of conduct, certification systems, regulatory decisions or guidelines apply to the planned data processing and take into account ethical considerations.

Involved parties

It is then necessary to identify which parties are involved in the data processing or the development and use of the system, service or product, and their role (e.g., controller or processor). Several parties may be jointly responsible for the data processing. Identifying the data controller, i.e., the party that alone or jointly with others decides the means and purposes of data processing, is essential to determine who is responsible and accountable for compliance with data protection requirements under the GDPR.

Legal justification

For all personal data processing, controllers must rely on one of the legal bases set out in Arts 6 and 9 of the GDPR, the most used of which are: legitimate interest; performance of a contract; legal obligation; or consent.

In health or medical apps collecting and processing special categories of patient or consumer data, the processing of this data will regularly require the data subjects explicit consent. In this case, consent must be voluntary and specific to each functionality that serves a distinct purpose. Consent must further be based on prior information. In the case of special categories of data, the use of cookies or location data, the data subject must provide explicit consent through positive action, such as downloading the app and ticking a consent box. Also, controllers must have a procedure in place that allows for easy withdrawal of consent and, on the other hand, ensures that in the event of withdrawal, the data collected will not be further processed.

Proportionality and data minimisation
Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed. This means that systems, apps and devices that store or process personal data should be set up so that only the data necessary for the individual purpose or the proper functioning of the system, app or device is stored and processed.

The principle of data minimisation can be achieved in different ways, for example, by reducing the amount of personal data collected and processed or by making it more difficult or impossible to assign the data to an individual.

Depending on the functionalities of the system, app or product and the purpose of the processing, the controller must therefore assess for each data set to be collected whether this data is indeed necessary to fulfil the purpose or whether the purpose can be fulfilled with less data (reduction of data volume) or pseudonymised/anonymised data (making identification difficult or impossible). A further distinction must be made between mandatory data and voluntary data that can be additionally provided for the use of certain functionalities.

Another measure that the controller can take to achieve the data minimisation requirement is to prevent the linking of personal data stored in different systems for different purposes.

Transparency and fair processing
Personal data must be processed transparently and fairly. Data subjects should have full transparency and control over the processing of their data and understand what data is being processed, why, by whom, where and for how long, and how they can exercise their data protection rights. The processing of personal data should neither violate applicable laws, nor be unexpected to the data subject.

The privacy notice should be easily accessible to data subjects at any time, before the collection of personal data and throughout the processing. Users of apps, for example, should be notified before the download of the app. The notice should be easy to understand and, where appropriate, translated in different languages.

Confidentiality and access to personal data
Personal data must be kept strictly confidential and may only be provided or disclosed to individuals on a need-to-know basis to fulfil the legitimate purposes for which the data was collected.

Special attention is required for centralised data management systems. In this case, the controller should establish data access and restriction policies and limit the access through technical means.

Purpose limitation
Personal data shall only be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.

The controller should determine the processing purposes and communicate them to the data subjects. The functionalities of the system, app or product should be set up to ensure that personal data is only processed for these purposes. The controller must also determine who should have access to which data for which purposes and implement these regulations through technical measures as well as instructions, training and controls.

If the personal data is to be processed later for purposes other than those communicated, it should be anonymised, unless there is another legal basis for this secondary use. In any case, data subjects should be informed in advance about the use of their data for any secondary purpose and, unless there is another legal basis, their consent should be obtained.

Data quality
The personal data stored must be accurate and, where necessary, kept up to date, and all reasonable steps must be taken to ensure that inaccurate personal data is erased or rectified without delay.

The controller must have mechanisms in place to ensure that data is accurate at the time of collection and is not unlawfully altered thereafter. There must be a mechanism to correct or delete inaccurate data.

Data retention
Personal data must be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, unless regulatory or legal requirements necessitate a longer or shorter retention period.

The controller should establish a data retention and deletion policy and determine a retention period for each data set based on the purpose of the processing and, where applicable, legal and regulatory retention periods.

The controller must also define mechanisms, including automated solutions where appropriate, and responsibilities for the effective deletion of data. If the data cannot be deleted, it must be anonymised or, if this is not possible, pseudonymised.

Data security
Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate TOMs. These measures should include data integrity and confidentiality, availability, resilience and traceability, and ensure a level of security appropriate to the risk to the rights of data subjects.

Appropriate control access mechanisms and authentication measures should be embedded in the system infrastructure to detect and monitor unauthorised access to data. Personal data should be protected by strong and robust state-of-the-art encryption, both in transit and in storage. Special attention is required when data is stored in the cloud.

Privacy rights
Data subjects have various data protection rights, including the right to information, access, rectification and erasure, restriction of processing, data portability and the right to object to automated individual decision-making. They also have the right to complain to the competent supervisory authority if they feel their rights are being violated or their data is not adequately protected. The controller must define processes to ensure that data can be corrected, deleted or transferred at the data subjects' legitimate request. For apps in particular, the controller should consider whether users should be able to exercise their rights directly through the app, if necessary, by accessing the data and correcting or deleting it if inaccurate.

Data processing by third parties and cross-border data transfers
Depending on the roles of the contributors in the development, management and use of the system, app or product and the data processed, the controller must establish appropriate contractual obligations to ensure data protection.

Before sharing any personal data with a processor, the controller must verify that the processor implements appropriate TOMs to ensure compliance with the data protection requirements and data subjects' privacy rights.

If personal data is to be transferred to third parties outside the European Economic Area ("EEA") to a country without a formal adequacy decision by the European Commission,

appropriate safeguards, such as EU standard contractual clauses ("SCCs"), must be implemented to legitimise cross-border data transfers, unless an exemption pursuant to Art. 49 GDPR applies, such as the explicit consent of the data subject.

Before transferring the data, the controller, respectively the data exporter, must check whether the destination country ensures an adequate protection level equivalent to that in the EU. If this is not the case, the data exporter should consider storing and processing the data in the EU or an adequate country. If this is not an option, additional contractual, technical and organisational measures must be taken, such as pseudonymisation or encryption of the data while keeping the encryption key in the EU and separate from the service provider.

4 Conclusion

Consistent and sustainable compliance with data protection requires the strategic and conceptual integration of data protection principles in all business practices, the organisational structure, the development of rules, IT systems and products.

To fully exploit the benefits of new technologies and ensure their effectiveness, it is essential to embed fundamental data protection principles into the design of these solutions, taking into account organisational, process and system-related risks, as well as risks to the rights of data subjects.

PbD is not only required by the GDPR and partly by laws of other countries outside the EEA. It is a prerequisite for the effective and sustainable implementation of data protection, the basis for the smooth functioning of data protection management, and a critical factor in achieving the necessary trust of employees, customers, patients and consumers, public authorities, business partners and other stakeholders in the use of new technologies and the processing of their personal data.

Fig.1

Daniela Fábián Masoch is the founder and executive director of FABIAN PRIVACY LEGAL GmbH, a boutique law firm specialised in international, European and Swiss data protection law, governance, risk management and programme implementation. Daniela is a Swiss attorney-at-law, certified Privacy Professional and ISMS 27001 Lead Auditor, with 30 years of professional experience. She advises multinational companies in the EU, Switzerland and the USA on data protection and security issues in various industries, mainly in the pharmaceutical and medical device industries.

Daniela supports her clients in evaluating, developing, implementing and monitoring data protection strategies, governance models and global data protection programmes and data transfer mechanisms with a pragmatic approach.

Before starting her own company in 2015, Daniela held various positions at Novartis, most recently as Global Head of Data Privacy, where she was responsible for the Group's strategic direction on data privacy, as well as establishing, implementing and overseeing the global data privacy function, global data privacy management programme and binding corporate rules.

Daniela is a member of various data protection associations and a lecturer at FernUni Switzerland for the CAS Data Protection and at Swiss Health Quality Association ("shqa") for Digital Marketing.

FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

FABIAN PRIVACY LEGAL GmbH is a boutique law firm specialising in international, European and Swiss data protection law, governance, risk management and programme implementation.

Our strengths are the combination of expert knowledge and practical in-house experience, an excellent network with industry groups and data protection associations, and close cooperation with data protection, cybersecurity and cybercrime experts worldwide as well as corresponding law firms advising on local legal issues. We approach mandates with a global, solution-oriented and practical approach to deliver pragmatic and sustainable solutions.

Our clients are large and small companies in a wide range of industries, including pharmaceuticals, biotechnology and medical devices, technology, consumer goods, luxury goods, food and beverages, transport and logistics, automotive, insurance, financial institutions and the chemical industry.

www.privacylegal.ch

FABIAN PRIVACY LEGAL

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group