CONNECT

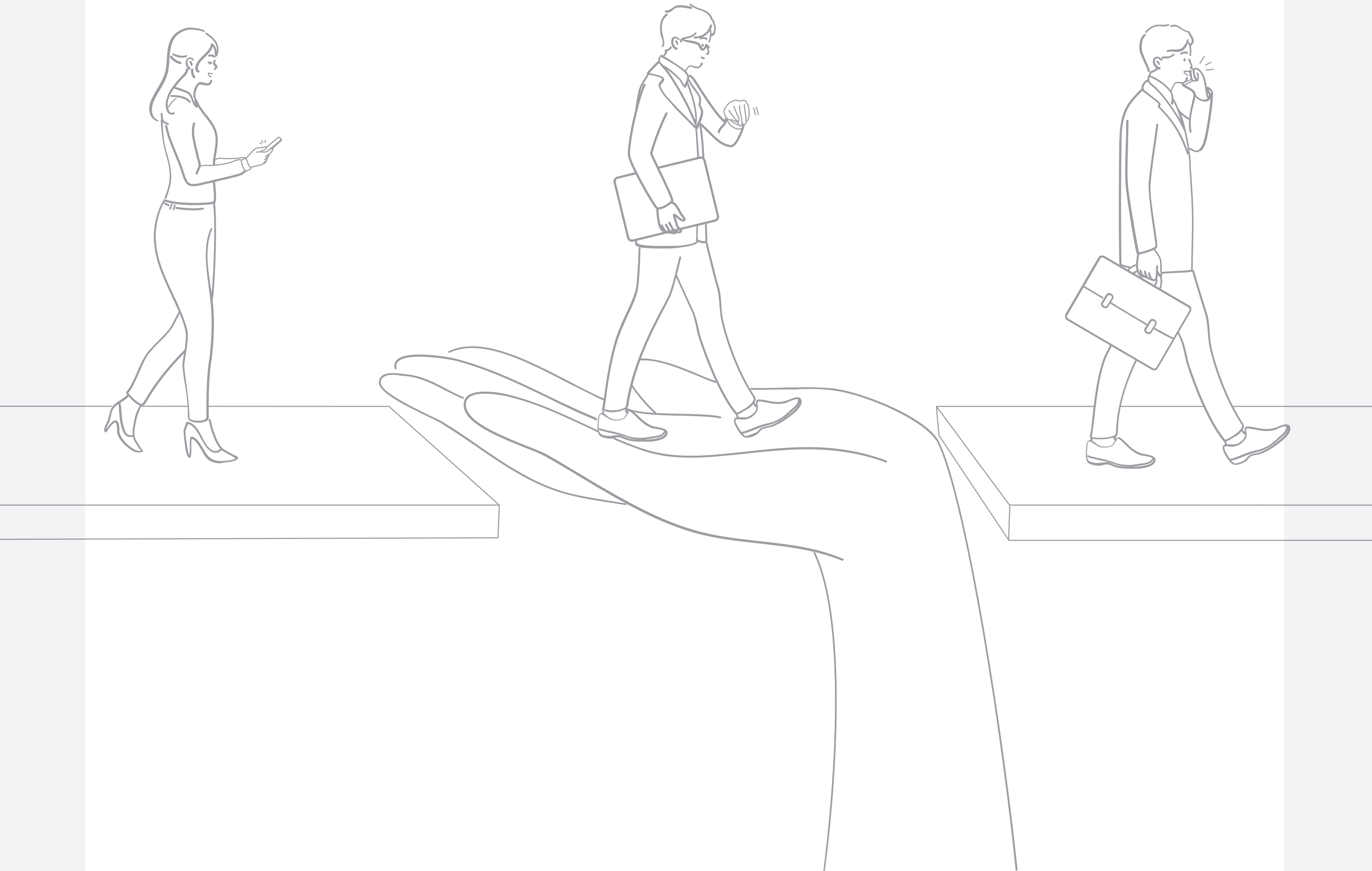
info@qprivacy.com

VISIT

www.qprivacy.com

DATA PROTECTION LEGISLATION, PRIVACY BY DESIGN, AND THIRD PARTY SDKS

How QPrivacy Protects Your Customers' Data and Ensures Regulatory Compliance



DATA PRIVACY LEGISLATION & PRIVACY BY DESIGN
AN OVERVIEW

According to the United Nations Conference on Trade and Development (UNCTAD), 66% of all countries in the world have enacted legislation to address data protection and privacy[1].

The General Data Protection Regulation, which became EU law in 2018, is arguably the most well-recognized and globally influential data protection legislation, and has outlined the following foundational principles of data protection:[2]

Lawfulness, Fairness, and Transparency: Any processing of personal data should be lawful and fair. It should be clear to users that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimisation: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date.

Storage Limitation: 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.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing, and against accidental loss, destruction or damage.

Accountability: The controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance.

These principles lay the groundwork for the other rules and obligations of the legislation, and are influencing legislation being drafted around the world. With more than 120 countries engaged in some form of international privacy laws for data protection, it is clear that this is a legal arena that will continue to evolve and mature.

7 Principles of Privacy by Design[3]

The principles above are critical for setting expectations, but are not sufficient for practical application. To that end, the GDPR places significant focus on Privacy by Design, a framework for building privacy into the design and operation of IT systems, networked infrastructure, and business practices. According to this framework, privacy management demands an interdisciplinary, systems engineering approach. Good privacy management encompasses:

- the full lifecycle of the data — from acquisition to use, storage, retention and disposal
- multiple teams with different objectives and priorities (e.g. product management and engineering, user support, sales and marketing, finance, risk and compliance)
- multiple control domains (e.g. technical, administrative, legal).

The 7 Privacy by Design principles are:

1. **Proactive not Reactive; Preventative not Remedial**
   By proactively adopting strong privacy practices, events which have an invasive effect on privacy are anticipated and prevented.

2. **Privacy as the Default Setting**
   Personal information is by default protected without the need for the user to take any action. The fair information practices – "Purpose Specification", "Collection Limitation", "Data Minimization", and "Use, Retention and Disclosure Limitation" – are taken into account.

3. **Privacy Embedded into Design**
   Privacy is considered in the design and architecture of IT systems and business practices as a core functionality. It should be embedded holistically in terms of considering the context, integrative as respecting all stakeholders, and creative as re-defining previous designs.

4. **Full Functionality – Positive-Sum, not Zero-Sum**
   All legitimate objectives of an organization are achieved with full functionality. A multi-functional solution is investigated where no trade-off is performed to the detriment of privacy.

5. **End-to-End Security – Full Lifecycle Protection**
   Strong security actions are taken throughout the entire lifecycle. The management of personal information and included principles are carried out, such as destroying data at regular intervals.

6. **Visibility and Transparency – Keep it Open**
   All stakeholders in business practices and technologies operating according the promises and objectives. For this, visibility and transparency are needed for establishing accountability and trust. In this principle, the three fair information practices – "Accountability, "Openness", and "Compliance" – are considered.

7. **Respect for the User – Keep it User Centric**
   The design should always consider the interests and needs of users. This principle implies the four fair information practices: "Consent" – users' consent regarding collection, usage, and disclosure of personal information; "Accuracy" – the need for complete, correct, and actual personal information; "Access" – providing user access to their data; and "Compliance" – interpreted as organizations having to take actions and communicating them regarding users' privacy.

Based on principles of Privacy by Design, governments are increasingly holding companies ("controllers") accountable for full protection of user data, regardless of where a data breach might occur. In fact, UNCTAD has noted a specific concern about "the collection, use and sharing of personal information to third parties without notice or consent of consumers."[4] Only by embedding privacy into the system from the outset, and carefully managing their data sharing with third parties, do companies today have any hope of effectively protecting user data.

[1] *UNCTAD, 02/04/2020. /Data Protection and Privacy Legislation Worldwide/ Accessed 24/8/202. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*

[2] *GDPR - Ireland, /https://www.dataprotection.ie/index.php/en/individuals/data-protection-basics/principles-data-protection*

[3] *Cavoukian, A. 2009. "Privacy by Design," Information and privacy commissioner of Ontario, Canada.*

[4] *UNCTAD, 02/04/2020. /Data Protection and Privacy Legislation Worldwide/*

ENFORCING DATA PRIVACY BY DESIGN FOR THIRD PARTIES

HOW QP HELPS YOU TAKE ACTION

QPrivacy's solution, as developed by Privacy Rating Ltd, covers substantial PbD and other regulatory requirements and concepts under privacy and data protection regulations worldwide, including Regulation (EU) 2016/679 (GDPR). The following are the broad PbD concepts and related principles addressed by QPrivacy, and descriptions of the activities QP uses to fulfill them, keeping your customers' data safe and your company fully compliant with the law, no matter where you do business or which third party SDKs you engage.

001

Concept	Data Minimization	
Principle	Collection [communications with the third parties]	
Activity	AVOIDANCE (Preventing third parties from collecting data)	
Activity Details	• The ability to 'filter' content in two manners: • identification of strings' structure such as government issued ID fields and blocking their transmission; and • managing specific parameters (i.e., key-values). • The client can define a POLICY and PREVENT specific predefined data from being collected by third parties (Data Avoidance) by blocking collection of content (attributes and identifiers) directly (strings) or through specific parameters. • In Incident and other relevant situations, the client can use a KILL SWITCH to completely block all collection of data by a third party.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

002

Concept	Data Minimization	
Principle	Collection [communications with the third parties]	
Activity	ACCESS LIMITATION (preventing third parties from accessing already collected data)	
Activity Details	• The ability to block access from defined destinations, e.g., URL blocking, or according to a third-party server ID. • The client can block access to data (user attributes and identifiers) by unknown or unauthorized third parties, and to block access to data (attributes and identifiers) by authorized third parties, who wish to access and transmit the data to unauthorized or unknown destinations. • In Incident and other relevant situations, the client can use a KILL SWITCH to completely block access to data to each third party. • The client can limit access to data by a new version of the third party SDK, by blocking or screening automated updates.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

003

Concept	Data Minimization	
Principle	Collection [communications with the third parties]	
Activity	DATA REUSE/REPURPOSING LIMITATIONS (preventing third parties from collecting data for further unintended or unauthorized use)	
Activity Details	• By obfuscating known parameters (data points), the client can prevent the collection of clear data by third parties, thereby preventing the third parties from repurposing the data for unauthorized purposes.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

004

Concept	Data Minimization	
Principle	Processing [processing of the data by third parties]	
Activity	ACCESS LIMITATION (limiting third parties' ability to process/use data)	
Activity Details	• The client can limit the processing of data (user attributes and identifiers) by authorized third parties, by preventing, obfuscating or encrypting data points. • In Incident and other relevant situations, the client can use a KILL SWITCH to completely block all further collection of, and access to data by a third party, thereby limiting third parties' ability to continue processing the collected data. • By limiting access to data by a new version of the third party SDK, through the blocking or screening of automated updates, the client can prevent unauthorized processing of data.	
QP Coverage	Web -- PARTIAL QP cannot intervene with user device run-time processing	Mobile -- PARTIAL QP cannot intervene with user device run-time processing
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

005

Concept	Data Minimization	
Principle	Processing [processing of the data by third parties]	
Activity	DATA REUSE/REPURPOSING LIMITATIONS (limiting third parties' unauthorized processing of clear data)	
Activity Details	• By obfuscating, hashing or encrypting data points, the client can prevent a third party from processing clear data, reusing or repurposing it.	
QP Coverage	Web -- PARTIAL QP cannot intervene with user device run-time processing	Mobile -- PARTIAL QP cannot intervene with user device run-time processing
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

006

Concept	Data Minimization	
Principle	Sharing [by the third parties with their sub-processors ("fourth parties")]	
Activity	DATA AVOIDANCE (minimizing the data that third parties collect and thereafter share with their sub-processors)	
Activity Details	• The ability to 'filter' content in two manners: (i) identification of strings' structure such as government issued ID fields and blocking their transmission; and (ii) managing specific parameters (i.e., key-values) . • Limiting clear data accessible by a third party, by defining a POLICY, also limits the third party's ability to share the data with other third parties (the third party's vendors, clients and partners).	
QP Coverage	Web -- PARTIAL QP cannot intervene with Server-to-Server communication	Mobile -- PARTIAL QP cannot intervene with Server-to-Server communication
Regulatory/Business Importance	Websites -- MEDIUM	Mobile Apps -- MEDIUM

007

Concept	Data Minimization	
Principle	Sharing [by the third parties with their sub-processors ("fourth parties")	
Activity	ACCESS LIMITATION (minimizing the already collected data that third parties can access and thereafter share with their sub-processors)	
Activity Details	• The client can limit the processing of data (user attributes and identifiers) by authorized third parties, by preventing, obfuscating or encrypting data points. • In Incident and other relevant situations, the client can use a KILL SWITCH to completely block all further collection of, and access to data by a third party, thereby limiting third parties' ability to continue processing the collected data. • By limiting access to data by a new version of the third party SDK, through the blocking or screening of automated updates, the client can prevent unauthorized processing of data.	
QP Coverage	Web -- PARTIAL QP cannot intervene with user device run-time processing	Mobile -- PARTIAL QP cannot intervene with user device run-time processing
Regulatory/Business Importance	Websites -- MEDIUM	Mobile Apps -- MEDIUM

008

Concept	Data Minimization	
Principle	Sharing [by the third parties with their sub-processors (“fourth parties”)]	
Activity	DATA REUSE/REPURPOSING LIMITATION (minimizing unauthorized processing of data by sub-processors)	
Activity Details	• Limiting clear data accessible by a third party, by defining a POLICY, also limits the third party's other parties (vendors, clients and partners) ability to access and use the data for unauthorized purposes. • By obfuscating third party cookies & identifiers, the client can prevent repurposing of the data through sharing the data with other parties.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH
Notes	Example: vendors (sub-processors) situated in unauthorized territories (e.g., for support purposes). By obfuscating third party cookies & identifiers, the client can prevent repurposing of the data through sharing the data with other parties.	

009

Concept	Audit, Control and Report	
Principle	Control	
Activity	SUPERVISION -- PERIODICAL/ON-GOING/REAL-TIME	
Activity Details	• Always-On, Real-Time special ability to policy Enforcement and Alerts	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

010

Concept	Audit, Control and Report	
Principle	Control	
Activity	AUDIT TRAIL	
Activity Details	• Periodical audit reports provide the client an ability to review and control the functioning of the pre-defined policies.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

011

Concept	Audit, Control and Report	
Principle	Control	
Activity	EVENT MONITORING	
Activity Details	• Audit trail detailed records by Event and per end-user.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

012

Concept	Audit, Control and Report	
Principle	Accountability	
Activity	RETRIEVABLE EVENT LOG FILES	
Activity Details	• Ability to demonstrate policy enforcement. Evidence of collection and Sharing per third party tool per parameter and per end-user.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

013

Concept	Audit, Control and Report	
Principle	Accountability (Demonstration of Compliance)	
Activity	RETRIEVABLE ACCESS LOG FILES	
Activity Details	• Ability to demonstrate unauthorized access. Evidence of collection and Sharing of data breach violations.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

014

Concept	Audit, Control and Report	
Principle	Accountability (Demonstration of Compliance)	
Activity	OTHER RECORDS AND DOCUMENTATION	
Activity Details	• Audit trail detailed records by Event and per end-user.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

015

Concept	Audit, Control and Report	
Principle	Data Breach Management and Mitigation	
Activity	INCIDENT MANAGEMENT	
Activity Details	• Alert, evidence and detailed reports regarding data breach and transfer to an unauthorized destination in total and per end-user.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

016

Concept	Audit, Control and Report	
Principle	Data Breach Management and Mitigation	
Activity	DATA SEGREGATION	
Activity Details	• Segregation by using different encryption allows data use on a need to know basis.	
QP Coverage	Web -- PARTIAL - not including data Silo	Mobile -- PARTIAL - not including data Silo
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

017

Concept	Audit, Control and Report	
Principle	Data Breach Management and Mitigation	
Activity	REDUCTION OF RISKS ASSOCIATED WITH DATA BREACHES	
Activity Details	• Risk reduction of Data Breaches on third parteis's systems through data control, content collection and access avoidance, limits data collection, access, repurposing and sharing of the data.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

018

Concept	Audit, Control and Report	
Principle	Data Breach Management and Mitigation	
Activity	REMOTE CONTROL OVER DATA ACCESS	
Activity Details	• Ability to avoid risks by blocking access to unauthorized or unknown URLs including the prevention of phishing attempts in web and redirect in mobile.	
QP Coverage	Web -- PARTIAL - not including defacement	Mobile -- PARTIAL - not including defacement
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

019

Concept	Audit, Control and Report	
Principle	Data Breach Management and Mitigation	
Activity	SEGREGATION OF CLIENTS' DATA	
Activity Details	• Ability to partial segregation using 3 different Encryption layers.	
QP Coverage	Web -- PARTIAL - not including Re-route	Mobile -- PARTIAL - not including Re-route
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

020

Concept	Audit, Control and Report	
Principle	Data Transfer	
Activity	SUPPLEMENTAL SAFEGUARDS	
Activity Details	• Encrypt data transfer by maintaining the private key in an adequate territory. • Ability to demonstrate that clear data is not accessible in unauthorized territories.	
QP Coverage	Web -- FULL for on-device communication (data in transit and data at rest).	Mobile -- FULL for on-device communication (data in transit and data at rest).
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

021

Concept	Audit, Control and Report	
Principle	Secure Data Cycle	
Activity	ISMS AREA - VENDOR MANAGEMENT	
Activity Details	• Third Party (vendors) Risk prevention and risk management - Management of risk associated with unauthorized Access and Data leakage to privileged vendors and non-privileged factors.	
QP Coverage	Web -- FULL for third parties in digital channels	Mobile -- FULL for third parties in digital channels
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

022

Concept	Audit, Control and Report	
Principle	Secure Data Cycle	
Activity	STATE OF THE ART (BEST AVAILABLE) TOMS	
Activity Details	• Appropriate technical and organizational measures (TOMs) to prevent unauthorized data leakage and Access. Best Available, in terms of vendors management, requires that the client will not rely solely on contracts with vendors and occasional vendor audits, but instead engage vendor management pro-actively and use PbD tools such as QPrivacy to manage and control data sharing with vendors on an on-going and real time basis.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- MEDIUM	Mobile Apps -- MEDIUM

023

Concept	Audit, Control and Report	
Principle	Secure Data Cycle	
Activity	ISMS AREA - INCIDENT MANAGEMENT	
Activity Details	• Assistance with incident management - data (records, logs, reports) for forensics + KILL SWITCH for mitigation.	
QP Coverage	Web -- FULL for on-device communication (data in transit and data at rest).	Mobile -- FULL for third parties in digital channels
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

024

Concept	Audit, Control and Report	
Principle	User-centric	
Activity	DATA SUBJECT RIGHTS (DSR)	
Activity Details	• DSAR (especially CCPA) - ability to provide the individual with information about the data collected by third parties (historically, and not just a current snapshot that anyone can draw from the F12 browser function).	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- HIGH	Mobile Apps -- HIGH

025

Concept	Audit, Control and Report	
Principle	User-centric	
Activity	CHOICE (CONSENT)	
Activity Details	• Consent Management Platform (CMP) by destination, parameter and content.	
QP Coverage	Web -- FULL	Mobile -- FULL
Regulatory/Business Importance	Websites -- MEDIUM	Mobile Apps -- MEDIUM