ADP Privacy Code for Business Data Overview

Introduction

ADP has adopted Binding Corporate Rules (BCR) as a Data Controller. BCR are a legally binding set of internal rules, recognized by the European Union (EU) Data Protection Authorities (DPAs), to ensure a consistent approach to privacy and data protection across Group Companies with the same parent, including those located outside of the EU.

Scope and Applicability

The ADP Privacy Code for Business Data indicates the commitments ADP has implemented for Processing Personal Data pertaining to those Individuals with whom ADP has a business relationship (e.g., Individuals who represent ADP's Clients, Suppliers and Business Partners, other Professionals, and Consumers) and other Individuals whose Personal Data are Processed by ADP in the context of its business activities as a Data Controller.

Implementation

The effective date of the ADP Privacy Code for Business Data is April 11, 2018. ADP will implement the ADP Privacy Code for Business Data across the relevant ADP Group Companies within 18 months of the effective date.

Glossary for BCR

To access the glossary of terms used throughout ADP BCR related materials, please click here.

ADP Business Data Code Principles

The ADP Privacy Code for Business Data is based on a set of data protection principles outlined below.

Business Purposes for Processing Personal Data

Personal Data may be Processed by ADP in the context of its business operations for one or more of the following Business Purposes:

A. Business Purposes for Processing Personal Data pertaining to Professionals:

1. Business relationship management;
2. Business relationship due diligence;
3. Transactional communications;
4. Account management;
5. Quality control;

6. Risk management;
7. Security management; and
8. Anonymize or de-identify Personal Data.

B. Business Purposes for Processing Personal Data pertaining to Consumers and other Individuals:

1. Provide requested information, products or services;
2. Due diligence;
3. Transactional communications;
4. Account management;
5. Risk management;
6. Security management; and
7. Anonymize or de-identify Personal Data.

C. Business-necessary Processing activities:

1. Protect privacy and security;
2. Treasury operations and money movement activities;
3. Compliance;
4. Business structuring activities; and
5. Reporting and analysis.

D. Development and improvement of products and/or services; and

E. Relationship management and marketing.

If a Business Purpose does not exist (or if Applicable Law so requires it), ADP shall seek consent from the Individual for the Processing. Individuals may withdraw consent at any time by giving notice to ADP.

Use for Other Purposes

Personal Data may be Processed for a Secondary Purpose, similar to the legitimate Business Purpose, provided appropriate additional measures are taken. It is generally permissible to Process Personal Data for the following purposes (even if not listed as a Business Purpose), provided appropriate additional measures are taken:

1. Disaster recovery and business continuity, including transferring the Information to an Archive;
2. Internal audits or investigations;
3. Implementation or verification of business controls;
4. Statistical, historical, or scientific research;
5. Dispute resolution;
6. Legal or business counseling;
7. Compliance with laws and company policies; or
8. Insurance purposes.

Purposes for Processing Special Categories of Data

The following Special Categories of Data may be Processed by ADP for the purposes specified below:

1. **Special Categories of Data revealed by Photographic Images**. Photographic images and video recordings may be Processed for security, compliance and other legitimate Business Purposes, such as participating in video conferences.
2. **Racial or ethnic data**. ADP may Process racial and ethnic data as needed to facilitate Supplier and other diversity programs.
3. **Criminal data** (including data relating to criminal behavior, criminal records, or proceedings regarding criminal or unlawful behavior). ADP may Process criminal data as needed to conduct appropriate due diligence on Individuals and in connection with security and compliance activities as needed to protect the interests of ADP.
4. **Physical or mental health data**. ADP may Process physical or mental health data as needed to accommodate a person's disability or dietary needs, address emergency health needs, or in similar circumstances.
5. **Biometric data** (such as fingerprints). ADP may Process biometric data for the protection of ADP and Staff assets, system and site access, security and fraud prevention reasons.
6. **Religion or beliefs**. ADP may Process data pertaining to religion or beliefs as needed to meet an Individual's specific needs, such as accommodating dietary requests (for kosher or halal meals) or respecting religious holidays.

Special Categories of Data may be Processed for any other legitimate purpose, if ADP obtains the prior explicit consent of the Individual.

ADP Privacy Code for Business Data Overview

Quantity and Quality of Data

ADP shall establish and implement retention schedules so that records containing Personal Data are only retained as needed to fulfill the applicable Business Purposes, to comply with applicable legal requirements, or as advisable in light of applicable statutes of limitations.

Personal Data should be accurate, complete, and kept up-to-date to the extent reasonably necessary for the applicable Business Purposes. It is the responsibility of Individuals to ensure that their Personal Data are accurate, complete, and up-to-date.

Individual Rights of Access, Rectification and Objection

Individuals have the right to request a copy of the Personal Data maintained by or on behalf of ADP. If the Personal Data are incorrect, incomplete, or not Processed in compliance with Applicable Law or the ADP Privacy Code for Business Data, the Individual has the right to have the Personal Data rectified, restricted or erased (as appropriate).

Additionally, Individuals have the right to object to a) the Processing of their Personal Data on the basis of compelling grounds related to their particular situation, or b) receiving direct marketing communications (opting-out).

Information around the process for submitting an Individual Rights Request can be found in Article 7 of the ADP Privacy Code for Business Data.

Security and Confidentiality Requirements

ADP has implemented commercially reasonable and appropriate technical, physical, and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access.

Access to Personal Data will be authorized only to the extent necessary to serve the applicable Business Purposes and ADP Staff with access to Personal Data will be subject to confidentiality obligations.

ADP shall investigate all known or suspected Data Security Breaches and shall document the facts relating thereto, its effects and the remedial actions taken. ADP shall notify Individuals of a Data Security Breach within a reasonable period of time following determination of such Data Security Breach if (a) the Individual is at a high risk of harm as a result of the Data Security Breach or, (b) (even if the Individual is not at a high risk of harm), if an applicable breach notification law requires Individual notification.

Direct Marketing

ADP respects the choices of Individuals and provides Individuals the choice to opt-in and opt-out of direct marketing. ADP will send direct marketing materials if the Individual has provided opt-in consent or if Applicable Law permits ADP to send marketing communications without explicit consent based on an existing business relationship.

ADP Privacy Code for Business Data Overview

Transfer of Personal Data to Third Parties and Internal Processors

ADP may transfer Personal Data to a Third Party and to Internal Processors to the extent necessary to serve the applicable Business Purposes. ADP will only transfer Personal Data to a Third Party or to an Internal Processor if a written contract has been entered into with the ADP Group Company ensuring that the same level of data protection will be applied as described in the ADP Privacy Code for Business Data.

Governance

ADP's privacy program is managed by ADP's Global Chief Privacy Officer and the members of the Data Privacy and Governance Team. ADP has implemented a Privacy Network comprised of the members of the Data Privacy and Governance Team and other members of the Legal department, including compliance professionals, and Data Protection Officers, who are in charge of privacy compliance within their respective regions, countries, Business Units or Functional areas.

Additionally, Privacy Stewards are Executives who have been appointed by ADP senior leaders to implement and enforce compliance with ADP's privacy program within their respective Business Units or Functional areas. Privacy Stewards and selected members of the Privacy Network serve on ADP's Privacy Leadership Council, led by ADP's Global Chief Privacy Officer, to oversee privacy compliance at ADP.

Training

All ADP Staff with access to or responsibilities for Processing Personal Data are required to complete Global Data Privacy Training through ADP's Learning Management Platform.

Monitoring and Audit

ADP shall audit business processes and procedures that involve the Processing of Personal Data for compliance with the ADP Privacy Code for Business Data on a regular basis. Additionally, ADP will allow its Processing facilities to be audited by the Lead DPA and DPAs of an EEA Country, as defined in the ADP Privacy Code for Business Data.

The Global Chief Privacy Officer shall produce an annual report for the ADP Executive Committee on compliance with the ADP Privacy Code for Business Data, privacy, data protection risks, and other relevant issues.

Complaints Procedure

Individuals covered by the ADP Privacy Code for Business Data may file a written complaint if they suspect that a member(s) of the ADP Group Companies has violated the commitments made in the ADP Privacy Code for Business Data, as further defined in the ADP Privacy Code for Business Data.

Complaints must be submitted in writing to the ADP Global Data Privacy and Governance Team. Complaints may be submitted via email to privacy@adp.com or via mail to:

ADP Privacy Code for Business Data Overview

ADP Delegated Entity

ADP Nederland B.V.

Lylantse Baan 1, 2908

LG CAPELLE AAN DEN IJSSEL

THE NETHERLANDS

Individuals may also file a complaint or claim with the relevant DPAs or the Courts.

ADP Privacy Code for Business Data

For the full text of the ADP Privacy Code for Business Data, please click here.

Contact Us

For more information about ADP's Privacy Program, including the ADP Privacy Code for Business Data, please contact the Global Data Privacy and Governance team at privacy@adp.com.