

ADP Privacy Code for Client Data Processing Services Overview



A more human resource.®

Introduction

ADP has adopted Binding Corporate Rules (BCR) as a Data Processor. 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.

The ADP Privacy Code for Client Data Processing Services indicates the commitments ADP has implemented for the Processing of Personal Data pertaining to Client Employees by ADP, in connection with providing Client Services and Client Support Activities.

Scope and Applicability

The ADP Privacy Code for Client Data Processing Services addresses the Processing of Personal Data of Client Employees by ADP in its role as a Data Processor for Clients in the course of delivering Client Services, where such Personal Data are:

- (a) Subject to EEA Applicable Law (or were subject to EEA Applicable Law prior to the transfer of such Personal Data to a Group Company outside the EEA in a country which has not been deemed to provide an adequate level of data protection by competent EEA institutions);
- (b) Collected originally in the context of the activities of an EEA establishment of a Client;
- (c) Subject to EEA Data Transfer Restrictions;
- (d) Processed by ADP outside the EEA in a country which has not been deemed to provide an adequate level of data protection by competent EEA institutions; and
- (e) Processed pursuant to a Service Agreement that specifically provides that the ADP Privacy Code for Client Data Processing Services shall apply to such Personal Data.

Implementation

The effective date of the ADP Privacy Code for Client Data Processing Services is April 11, 2018. ADP will implement the ADP Privacy Code for Client Data Processing Services 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 Privacy Code for Client Data Processing Services Overview

ADP Privacy Code for Client Data Processing Services Principles

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

Data Processing Purposes

ADP shall Process Client Data on behalf of the Client, only in accordance with the Service Agreement, pursuant to any documented instructions received from the Client, or as needed to comply with Applicable Law.

ADP Processes Personal Data (including Special Categories of Data) pertaining to Client Employees as needed to provide Client Services, Client Support Activities, as required by EEA Applicable Law and for the following additional purposes:

- (a) Hosting, storage, and other Processing needed for business continuity and disaster recovery;
- (b) System and network administration and security, including infrastructure monitoring, identity and credential management, verification and authentication, and access control;
- (c) Monitoring and other controls needed to safeguard the security and integrity of transactions;
- (d) Enforcing contracts and protecting ADP, its Associates, Clients, Client Employees, and the public against theft, legal liability, fraud, or abuse; and
- (e) Approved ADP internal business processes.

Upon termination of the Service Agreement, ADP shall fulfill its obligations to the Client with regard to the returning the Data and securely destroying the Data, subject to EEA Applicable Law.

Security Requirements

ADP has implemented commercially reasonable and appropriate technical, physical, and organizational measures to protect Client Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access during the Processing, which will meet the requirements of EEA Applicable Law, or any stricter requirements, as imposed under the Service Agreement.

Access to Client Data will be authorized only to the extent necessary to serve the applicable Data Processing Purposes and requirements of the Service Agreements. ADP Staff with access to Client Data will be subject to confidentiality obligations.

ADP shall notify the Client of a Data Security Breach without undue delay after becoming aware that such a breach has occurred, unless a law enforcement official or supervisory authority determines that notification would impede a criminal investigation, or cause damage to national security or a breach of trust in the relevant industry sector.

ADP Privacy Code for Client Data Processing Services Overview

Transparency to Client Employees

ADP shall promptly notify the Client of requests or complaints related to the Processing of Personal Data by ADP that are received directly from Client Employees without responding to such requests or complaints, unless otherwise provided in the Service Agreement or instructed by the Client.

Subprocessors

Third Party Subprocessors may only Process Client Data pursuant to a Subprocessor Contract. The Subprocessor Contract shall impose similar data protection-related Processing terms on the Third Party Subprocessor that will be not less protective than those imposed on the ADP Contracting Entity by the Service Agreement and the ADP Privacy Code for Client Data Processing Services.

ADP shall publish an overview of the categories of Subprocessors involved in the performance of the relevant Client Services and ADP shall provide notice to the Client of any new Subprocessors engaged by ADP for the delivery of the Client Services. Clients have 30 days from notification date to object to the use of new Subprocessors engaged by ADP.

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.

Compliance

ADP shall respond promptly and appropriately to requests for assistance from the Client to enable the Client to comply with its obligations, subject to Applicable Law and in accordance with the Service Agreement.

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 will address Client audit requests and will answer questions asked by the Client regarding the Processing of Client Data by ADP. If further information is requested, in agreement with Client, ADP will either a) allow an independent third party assessor to conduct an audit, no more than annually per client, subject to a 45 day written notice and bound by confidentiality terms, or b) provide the Client with a statement from a third party assessor,

ADP Privacy Code for Client Data Processing Services Overview

indicating ADP's compliance with the ADP Privacy Code for Client Data Processing Services. Additionally, ADP will allow its Processing facilities to be audited by any DPA of an EEA Country which is competent to audit an ADP Client.

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

Complaints Procedure

Client Employees covered by the ADP Privacy Code for Client Data Processing Services 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 Client Data Processing Services, as further defined in the ADP Privacy Code for Client Data Processing Services.

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 Delegated Entity

ADP Nederland B.V.

Lylantse Baan 1, 2908

LG CAPELLE AAN DEN IJSSEL

THE NETHERLANDS

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

ADP Privacy Code for Client Data Processing Services

For the full text of the ADP Privacy Code for Client Data Processing Services, please click [here](#). For a list of the Group Companies bound by ADP's Privacy Code for Client Data Processing Services, please click [here](#).

Contact Us

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