ADP Privacy Code for Business Data

ADP Privacy Code for Business Data

Introduction

ADP has committed itself to the protection of Personal Data in the **ADP Code of Business Conduct and Ethics.**

This ADP Privacy Code for Business Data indicates how this commitment is implemented for ADP's Processing of 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.

For the rules applicable to ADP's Processing of Personal Data pertaining to its Associates, Contingent Workers and others for its own human resources purposes as a Data Controller, refer to the ***ADP Workplace Privacy Code***.

For the rules applicable to ADP's Processing of Personal Data pertaining to Client Employees on behalf of ADP's Clients as a Data Processor, refer to the ***ADP Privacy Code for Client Data Processing Services***.

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Professionals, Consumers, and other Individuals (such as investors) by ADP as a Data Controller in the course of ADP's business operations. This Code does not apply to the Processing of Personal Data of Individuals that is covered by the ADP Workplace Code. Where there is a question as to the applicability of this Code, the relevant Privacy Steward shall seek the advice of the Global Data Privacy and Governance Team before the Processing takes place.
Opt-out for Local-for-Local Processing	1.2	A Group Company not established in the EEA and not covered by an Adequacy Decision may opt-out of the applicability of this Code in respect of Processing of Personal Data collected in connection with the activities of such Group Company, provided such Personal Data are subsequently Processed in the relevant jurisdiction of such Group Company only and are not subject to the EEA Applicable Laws (Local-for-Local Processing). The opt-out by a Group Company for Local-to-Local Processing requires the prior authorization of the Global Chief Privacy Officer. Notwithstanding such an authorization, the Local-for-Local Processing shall at least be compliant with applicable local laws and the security and governance requirements of this Code.
Electronic and Paper-based Processing	1.3	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

Applicability of Local Law and Code 1.4 Nothing in this Code shall be construed to take away any rights or remedies that Individuals may have under Applicable Law. Where Applicable Law provides more protection than this Code, the relevant provisions of Applicable Law shall apply. Where this Code provides more protection than Applicable Law, or where it provides additional safeguards, rights, or remedies for Individuals, this Code shall apply.

Policies and Guidelines 1.5 ADP may supplement this Code through policies, standards, guidelines, and instructions that are consistent with this Code.

Accountability 1.6 This Code is binding upon ADP. The Responsible Executives shall be accountable for their business organizations' compliance with this Code. ADP Staff must comply with this Code.

Effective Date 1.7 This Code has been approved by the General Counsel, upon presentation by the Global Chief Privacy Officer, and has been adopted by the ADP Executive Committee and will enter into force as of 11 April 2018 (**Effective Date**). The Code shall be published on the www.adp.com website. It shall also be made available to Individuals upon request.

This Code shall be implemented by the ADP Group based on the timeframes specified in Article 22.

Prior Policies 1.8 This Code supplements ADP's privacy policies and supersedes previous statements to the extent they are in contradiction with this Code.

Role of ADP Delegated Entity 1.9 Automatic Data Processing, Inc. has appointed ADP Nederland B.V., having its registered seat in Lylantse Baan 1, 2908 LG CAPELLE AAN DENIJSSEL, The Netherlands, as the ADP Delegated Entity, in charge with enforcing this Code within the ADP Group, and ADP Nederland, B.V., has accepted this appointment.

Article 2 – Purposes for Processing Personal Data

Legitimate Business Purposes 2.1 Personal Data may be Processed by ADP in the context of its business operations for one or more of the following purposes (collectively, the **Business Purposes**):

(a) **Business Purposes for Processing Personal Data pertaining to Professionals.** Personal Data pertaining to Professionals with whom ADP has a business relationship may be Processed as needed:

(1) To initiate, assess, develop, maintain, or expand a business relationship, including negotiating, contracting, and fulfilling obligations under contracts;

(2) For due diligence regarding the Individual's qualifications and eligibility for the relationship, including verifying the identity, qualification, authority, and creditworthiness of the Professional and

obtaining publicly-available information from Third Parties (such as publicly-available sanction lists from screening companies);

(3) To send transactional communications (such as requests for information, responses to requests for information, orders, confirmations, training, and service updates);

(4) For account management, accounting, finance, and dispute resolution purposes (such as accounts receivable, accounts payable, account reconciliation, cash management, or money movement) and for consolidated management and reporting;

(5) To assure quality control and to enforce company standards and policies;

(6) For risk management and mitigation, including for audit and insurance functions, and as needed to license and protect intellectual property and other assets;

(7) For security management, including monitoring Individuals with access to ADP's websites, applications, systems, or facilities, investigation of threats, and as needed for any Data Security Breach notification; and

(8) To anonymize or de-identify the Personal Data.

(b) **Business Purposes for Processing Personal Data pertaining to Consumers and other Individuals.** Personal Data pertaining to Consumers and other Individuals with whom ADP has a business relationship may be Processed as needed:

(1) To provide the information, product, or service requested by the Individual, and as would be reasonably expected by the Individual given the context in which the Personal Data were collected, and the information provided in the applicable privacy statement given to the Individual (such as for personalization, remembering preferences, or respecting Individual rights);

(2) For due diligence, including verifying the identity of the Individual, as well as the eligibility of the Individual to receive information, products, or services (such as verifying age, employment, or account status);

(3) To send transactional communications (such as requests for information, responses to requests for information, orders, confirmations, training materials, and service updates);

(4) To manage the Individual's account, such as for customer service, finance, and dispute resolution purposes;

(5) For risk management and mitigation, including for audit and insurance functions, and as needed to license and protect intellectual property and other assets,

(6) For security management, including monitoring Individuals with access to ADP's websites, applications, systems, or facilities,

investigation of threats, and as needed for any Data Security Breach notification; and

(7) To anonymize or de-identify the Personal Data.

(c) **Business-necessary Processing activities.** ADP may Process Personal Data as needed (i) to protect the privacy and security of the Personal Data it maintains, such as in connection with advanced security initiatives and threat detection; (ii) for treasury operations and money movement activities; (ii) for compliance functions, including screening Individuals against sanction lists in connection with anti-money laundering programs; (iv) for business structuring activities, including mergers, acquisitions, and divestitures; and (v) business activities, management reporting, and analysis.

(d) **Development and improvement of products and/or services.** ADP may Process Personal Data to develop and improve ADP's products and/or services, and for research, development, analytics, and business intelligence.

(e) **Relationship management and marketing.** ADP may Process Personal Data for relationship management and marketing. This purpose includes sending marketing and promotional communications to Individuals who have not objected to receiving such messages as may be appropriate given the nature of the relationship, such as product and service marketing, investor communications, Client communications (*e.g.,* HR compliance alerts, product updates, and training opportunities and invitations to ADP events), customer satisfaction surveys, supplier communications (*e.g.,* requests for proposals), corporate communications, and ADP news.

Consent 2.2 If a Business Purpose does not exist (or if Applicable Law so requires it), ADP shall seek consent from the Individual for the Processing. Consent must be unambiguous, freely given, specific and informed. When seeking such consent to Process Personal Data, ADP must inform the Individual of the purpose(s) for which the Personal Data will be Processed and provide other relevant and legally-required information (*e.g.*, the nature and categories of the Processed Data, the categories of Third Parties to which the Data will be disclosed (if any), and how Individuals can exercise their rights to withdraw consent and that withdrawal of consent will not affect the lawfulness of the relevant Processing before such withdrawal).

Where Processing is undertaken at the Individual's request (*e.g.*, he or she subscribes to a service or seeks a benefit), he or she is deemed to have provided consent to the Processing for that purpose.

Denial or Withdrawal of Consent 2.3 When Processing is based on an Individual's consent, the Individual may deny consent, in which case the Personal Data shall not be Processed. Individuals may also withdraw consent at any time by giving notice to ADP.

In this case, ADP shall cease Processing the Personal Data as soon as practically possible. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its withdrawal; and (ii) the lawfulness of Processing for Business Purposes not based on consent after withdrawal.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

3.1 Personal Data shall be Processed only for the Business Purposes. Personal Data may be Processed for a legitimate Business Purpose other than the Business Purposes (a **Secondary Purpose**) only if the Secondary Purpose is closely-related to the Business Purpose(s).

Should any Group Company want to Process Personal Data for a Secondary Purpose, the relevant Privacy Steward shall consult with the Global Data Privacy and Governance Team.

Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Individual, the Processing may require additional measures such as:

(a) Limiting access to the Personal Data;

(b) Imposing additional confidentiality requirements;

(c) Taking additional security measures, including encryption or pseudonymization;

(d) Informing the Individual about the Secondary Purpose;

(e) Providing an opt-out opportunity; or

(f) Obtaining an Individual's consent in accordance with Article 2.2 or Article 4.3 (if applicable).

Generally Permitted Secondary Purposes

3.2 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 in accordance with Article 3.1:

(a) Disaster recovery and business continuity, including transferring the Information to an Archive;

(b) Internal audits or investigations;

(c) Implementation or verification of business controls;

(d) Statistical, historical, or scientific research;

(e) Dispute resolution;

(f) Legal or business counseling;

(g) Compliance with laws and company policies; or

(h) Insurance purposes.

Article 4 – Purposes for Processing Special Categories of Data

Specific Purposes for Processing Special Categories of Data

4.1 This Article sets forth specific rules for Processing Special Categories of Data. ADP shall Process Special Categories of Data only to the extent necessary to serve the applicable Business Purpose.

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

(a) **Special Categories of Data revealed by Photographic Images.** ADP recognizes that photographic images and video recordings may reveal Special Categories of Data (such as racial or ethnic information, physical health information and disabilities, and religious inclinations). ADP may view, collect, and otherwise Process images as reasonably needed for security and compliance purposes (such as for identification/authentication or premise monitoring activities). ADP may also Process images for other legitimate business reasons, such as when Individuals participate in video conferences.

(b) **Racial or ethnic data.** ADP may Process racial and ethnic data as needed to facilitate Supplier and other diversity programs.

(c) **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, its Staff, Clients, Client Employees, Business Partners, and Individuals against injury, fraud, theft, liability, or abuse. For example, ADP will investigate allegations of identify fraud as needed to protect itself, its Clients, and Individuals.

(d) **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. ADP may also Process heath data for accessibility purposes, such as working with visually-impaired Individuals to ensure that ADP's software products interact properly with screen reader technology, or as otherwise needed to enable Individuals to use its products and services.

(e) **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;

(f) **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.

General Purposes for Processing of Special Categories of Data

4.2 In addition to the specific purposes listed in Article 4.1 above, Special Categories of Data may be Processed:

(a) As permitted by law, such as for the performance of a task carried out to comply with a legal obligation;

(b) For the establishment, exercise, or defense of a legal claim;

(c) To protect a vital interest of an Individual, but only where it is impossible first to obtain the Individual's consent; or

(d) If the Special Categories of Data have manifestly been made public by the Individual.

Other Purposes for Processing of Special Categories of Data

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

Denial or Withdrawal of Consent

4.4 If ADP seeks consent from the Individual for the Processing of Special Categories of Data, the requirements set out in Article 2.2 and Article 2.3 above shall apply to the denial or withdrawal of consent.

Prior Authorization

4.5 Where Special Categories of Data are Processed based on a requirement of law other than the Applicable Law to the Processing, or pursuant to consent obtained in accordance with Article 4.3, the Processing requires the prior authorization of the Global Data Privacy and Governance Team.

Secondary Purposes

4.6 Special Categories of Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3.

Article 5 – Quantity and Quality of Data

No Excessive Data

5.1 ADP shall restrict the Processing of Personal Data to those data elements that are reasonably adequate for and relevant to the applicable Business Purposes.

Retention Periods

5.2 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.

Promptly after the applicable retention period has ended, the relevant business unit or functional area will take one of the following steps:

(a) Securely delete or destroy the Personal Data;

(b) De-identify the Personal Data; or

(c) Transfer the Personal Data to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Data 5.3 Personal Data should be accurate, complete, and kept up-to-date to the extent reasonably necessary for the applicable Business Purposes. ADP shall update Personal Data as needed to maintain the quality of the data and shall refrain from Processing any Personal Data that is not of appropriate quality for the applicable Business Purpose.

Privacy by Design 5.4 ADP shall take commercially reasonable technical and organizational steps to ensure that the requirements of this Article 5 are implemented into the design of new systems and processes that Process Personal Data.

Accuracy of Data 5.5 It is the responsibility of Individuals to ensure that their Personal Data are accurate, complete, and up-to-date. Individuals shall inform ADP of any changes to their Personal Data in accordance with Article 7.

Article 6 – Individual Information Requirements

Information Requirements 6.1 ADP shall publish privacy statements to inform Individuals about:

(a) The Business Purposes (including Secondary Purposes) for which their Personal Data are Processed;

(b) The Group Companies responsible for the Processing;

(c) The categories of Third Parties to which the Personal Data are disclosed (if any) and, (if applicable) whether a Third Party is not covered by an Adequacy Decision; and

(1) Other relevant information, such as the nature and categories of the Personal Data and how Individuals can exercise their rights;

(d) A contact person to whom requests under Article 7.1 can be addressed.

If EEA Applicable Law so requires, ADP will provide the relevant Individuals with the following additional information:

(a) the period for which the Personal Data will be stored or (if not possible) the criteria used to determine this period;

(b) an overview of the rights of Individuals under this Code, how these can be exercised, including the right to obtain compensation;

(c) the existence of automated decision making referred to in Article 10 as well as meaningful information about the logic involved and potential negative consequences thereof for the Individual;

(d) the source of the Personal Data (where the Personal Data have not been obtained from the Individual), including whether the Personal Data came from a public source.

(e) When Personal Data are transferred to a Third Party not covered by an Adequacy Decision, information on the data transfer mechanism as

referred to in Article 11.6(b), (c) and (d) as well as the means to get a copy of thereof or where these have been made available to Individuals.

Personal Data Not Obtained from the Individual

6.2 If Applicable Law so requires, where Personal Data have not been obtained directly from the Individual, ADP shall provide the Individual with the information set out in Article 6.1:

(a) At the time that the Personal Data are recorded in an ADP database;

(b) Within a reasonable and legally permitted period after collection, considering the specific circumstances of Personal Data collection and the Processing Purposes;

(c) At the time that the Personal Data are used for a mailing or other communication with the Individual; or

(d) If a disclosure to another recipient is envisaged, at the latest when Personal Data are first disclosed to the recipient.

Exceptions

6.3 The requirements of Articles 6.1 and 6.2 may be set aside if:

(a) The Individual already has the information as set out in Article 6.1; or

(b) It would be impossible, or would involve a disproportionate effort to provide the information to Individuals;

(c) Obtaining Personal Data is expressly laid down in Applicable Law; or

(d) The information is confidential or subject to an obligation of professional secrecy regulated by Applicable Law, including a statutory obligation of secrecy.

These exceptions to the above requirements qualify as Overriding Interests.

Article 7 – Individual Rights of Access, Rectification and Objection

Rights of Individuals

7.1 Individuals have the right to request a copy of the Personal Data maintained by or on behalf of ADP. Where reasonably possible, the overview shall contain information regarding the source of the Personal Data, the nature of the data elements, the purposes for which the Personal Data are Processed, and the categories of recipients of the Personal Data (if any).

If the Personal Data are incorrect, incomplete, or not Processed in compliance with Applicable Law or this Code, the Individual has the right to have the Personal Data rectified, restricted or erased (as appropriate).

In case the Personal Data have been made public by ADP, and the Individual is entitled to deletion of the Personal Data under EEA Applicable Law, in addition to deleting the relevant Personal Data, ADP shall take commercially reasonable steps to inform Third Parties that are Processing the relevant Personal Data or linking to the relevant Personal Data, that the Individual has requested the deletion of the Personal Data by such Third parties.

In addition, the Individual has the right to object to:

(a) The Processing of his or her Personal Data on the basis of compelling grounds related to his or her particular situation, unless ADP can demonstrate a prevailing legitimate interest for the Processing; and

(b) Receiving marketing communications on the basis of Article 9.3 (including any profiling based thereon).

Individuals may also raise with ADP any data protection right they benefit under Applicable Law.

When a request or objection is justified, ADP will take steps to rectify, restrict, or erase the relevant Personal Data or cease the relevant Processing (as appropriate) within the time period required by Applicable Law.

Procedure

7.2 Individuals should send their requests to the contact person indicated in the relevant privacy statement. Individuals may also send their requests to ADP's Global Data Privacy and Governance Team via email to privacy@adp.com.

Prior to fulfilling Individuals' requests for access to Personal Data, ADP may require the Individuals to specify their request when needed to provide an adequate response:

(a) Specify for example, to the extent reasonably possible, the concerned categories of Personal Data, the data system, business unit or functional area;

(b) Specify the circumstances in which ADP obtained the Personal Data;

(c) Provide proof of identity (if applicable) or provide additional information enabling identification;

(d) Pay a fee to compensate ADP for the reasonable costs relating to fulfilling the request provided ADP can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character; and

(e) In the case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Data are incorrect, incomplete, or not Processed in accordance with Applicable Law or this Code.

Response Period

7.3 Within four weeks of ADP receiving the request, the Global Data Privacy and Governance Team shall inform the Individual in writing either (i) of ADP's position with regard to the request and any action ADP has taken or will take in response, or (ii) the ultimate date on which the Individual will be informed of ADP's position and the reasons for the delay, which date shall be no later than eight weeks thereafter.

Complaint

7.4 An Individual may file a complaint in accordance with Article 17.3 and/or file a complaint or claim with the authorities or the courts in accordance with Article 18 if:

(a) ADP's response to the request is unsatisfactory to the Individual (*e.g.*, the request is denied);

(b) The Individual has not received a response as required by Article 7.3; or

(c) The time period provided to the Individual in accordance with Article 7.3 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which the Individual will receive a response.

Denial of Requests

7.5 ADP may deny an Individual's request if:

(a) The request does not meet the requirements of Articles 7.1 and 7.2;

(b) The request is not sufficiently specific;

(c) The identity of the relevant Individual cannot be established by reasonable means;

(d) It is impossible to provide the information, or if providing such information would require a disproportionate effort or result in a disproportionate expense that is not outweighed by the rights and interests of the Individual;

(e) Where Personal Data must remain confidential, subject to an obligation of professional secrecy regulated by Applicable Law, including a statutory obligation of secrecy;

(f) ADP can reasonably demonstrate that the request is unreasonable or excessive depending on the circumstances specific to the Individuals, such as in the event of repetitive requests. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval;

(g) The Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of ADP;

(h) The Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;

(i) The Processing is necessary for exercising the right of freedom of expression and information;

(j) For dispute resolution purposes;

(k) In so far as the request violates the rights and freedoms of ADP or others; or

(l) In case a specific restriction of the rights of Individuals applies under Applicable Law.

Not Required to Process Information

7.6 ADP is not obliged to Process additional information in order to be able to identify the Individual for the sole purpose of facilitating the rights of the Individual under this Article 7.

Article 8 – Security and Confidentiality Requirements

Data Security 8.1 ADP shall employ appropriate, commercially-reasonable technical, physical, and organizational measures to protect Personal Data from misuse and from accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access. To achieve this, ADP has developed and implemented a comprehensive information security program that is implemented through various policies, standards and controls, and that addresses the confidentiality, integrity, and availability of Personal Data with enhanced protection afforded to Special Categories of Data and other sensitive data elements.

The ADP Security, Risk and Privacy Policies and Standards are available to Staff via the ADP's Global Management Policy Platform on ADP's Associate web portals.

Staff Access 8.2 Staff shall be authorized to access Personal Data only to the extent necessary to serve the applicable Business Purposes.

Confidentiality Obligations 8.3 Staff who access Personal Data must meet ADP's confidentiality obligations.

Data Security Breaches 8.4 ADP shall investigate all known or suspected Data Security Breaches and shall document the facts relating thereto, its effects and the remedial actions taken, which documentation will be made available to the Lead DPA and a DPA competent to audit under Article 16.2 upon request. Group Companies shall inform the Global Chief Privacy Officer of a Data Security Breach without delay. 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. ADP may delay notification if a law enforcement or other regulatory authority determines that notification would impede a criminal investigation or cause damage to national security. In this case, notification shall be delayed as instructed by such authority. ADP shall respond promptly to inquiries of Individuals and Data Protection Authorities relating to such Data Security Breach.

Article 9 – Direct Marketing

Direct Marketing 9.1 This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (*e.g.*, contacting the Individual by email, fax, phone, SMS, or otherwise, to offer the opportunity to purchase goods or services from ADP).

Consent for Direct Marketing 9.2 If Applicable Law so requires, ADP shall send to Individuals unsolicited marketing communication with the prior consent of the Individual ("opt-in"). If Applicable Law does not require prior consent of the Individual, ADP shall

respect the Individual's right to opt-out of receiving unsolicited marketing communications.

If Applicable Law permits ADP to send marketing communications without explicit consent based on an existing business relationship, ADP may use this exception.

Information to be Provided 9.3 Every direct marketing communication shall provide the Individual with the opportunity and information about how to opt-out of further direct marketing communications.

Objection to Direct Marketing 9.4 If an Individual objects to receiving marketing communications from ADP, or withdraws consent to receive such materials, ADP will take steps to refrain from sending further marketing materials as specifically requested by the Individual. ADP will do so within the time period required by Applicable Law.

Third Parties and Direct marketing 9.5 ADP shall not allow Third Parties to use Personal Data for their own direct marketing purposes without the prior consent of the Individual.

Professionals that utilize services from ADP Marketplace Business Partners (or other partners who provide services directly to ADP Clients) may provide their consent for data sharing with and direct marketing from those Business Partners in the course of utilizing such services.

Marketing to Children 9.6 ADP shall not use any Personal Data of Children for direct marketing, without the prior consent of their parent or guardian.

Direct Marketing Records 9.7 ADP shall keep records reflecting Individual marketing preferences as needed to comply with this Article 9. Where required by Applicable Law or industry standards, ADP will update its records to reflect publicly-maintained suppression list data, such as government-mandated no-call lists. These records may be maintained at the corporate business unit or functional area level, as appropriate.

Article 10 – Automated Decision Making

Automated Decisions 10.1 ADP will comply with all Applicable Laws that regulate automated decision-making. Where such laws restrict the use of automated decision-making tools, ADP will not make adverse decisions about an Individual solely based on the results provided by the automated tool unless:

(a) The use of the automated decision-making tool is necessary to comply with a legal obligation (such as automated screening against watch lists) or to protect the interests of ADP, its Staff, Clients, Client Employees, Business Partners, or Individuals (such as automated fraud detection and suspicious transaction blocking);

(b) The decision is made by ADP for purposes of entering into or performing a contract, provided suitable measures are taken to safeguard the privacy

and legitimate interests of the Individual (*e.g.*, the Individual has been provided with an opportunity to express his or her point of view); or

(c) The decision is made based on the explicit consent of the Individual.

Items (a) and (c) only apply if suitable measures are taken to safeguard the legitimate interests of the Individual (e.g., the Individual has been provided with an opportunity to express his or her point of view).

Article 11 – Transfer of Personal Data to Third Parties and Internal Processors

Transfer to Third Parties

11.1 This Article sets forth requirements concerning the transfer of Personal Data from ADP to a Third Party. For purposes of this Article, "transfer" includes transmitting Personal Data to Third Parties as well as enabling Third Parties to remotely access such Personal Data maintained by ADP.

Categories of Third Parties

11.2 There are two categories of Third Parties: Third Party Controllers and Third Party Processors.

Transfer for Applicable Business Purposes Only

11.3 ADP may transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purposes (as well as Secondary Purposes per Article 3, or purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller Contracts

11.4 Third Party Controllers may Process Personal Data only if they have a written or electronic agreement with ADP. In the agreement, ADP shall safeguard the data protection interests of Individuals when Personal Data are transferred to Third Party Controllers. The Global Data Privacy and Governance Team shall provide guidance on these agreements. This requirement shall not apply to disclosures to Third Parties Controllers that are:

(a) Directly subject to a legal obligation to provide adequate protection for the Personal Data;

(b) Required by law (such as disclosures to government agencies); or

(c) Made at the direction of the Individual (such as pursuant to an Individual's request that ADP provides the Individual's information to another company in order to enable the company to provide integrated service information directly to the Individual).

Third Party Processor Agreements

11.5 Third Party Processors may Process Personal Data only if they have a written or electronic agreement with ADP (**Processor Contract**). The agreement with the Third Party Processor must include at a minimum, in compliance with Applicable Law, provisions which will address the following:

(a) The Third Party Processor shall Process the Personal Data only in accordance with ADP's instructions and for purposes authorized by ADP;

(b) The Third Party Processor shall keep the Personal Data confidential;

(c) The Third Party Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;

(d) Other than as expressly needed to perform the services, the Third Party Processor shall not permit subcontractors to Process the Personal Data without the prior written consent of ADP;

(e) ADP may review and verify the security measures taken by the Third Party Processor. Where required by law (and subject to appropriate conditions), the Third Party Processor shall at ADP's option (i) subject its relevant data processing facilities to audits and inspections by ADP, a third party assessor on behalf of ADP, or any relevant government authority, or (ii) provide ADP a statement issued by a qualified independent third party assessor certifying that the Processor has implemented appropriate technical and organizational security controls at its data processing facilities;

(f) The Third Party Processor shall promptly (i) respond to any inquiries from ADP regarding its Processing activities; (ii) provide assistance to ADP to address any DPA query and to perform required DPA formalities on the basis of the information available to the Third Party Processor and (iii) inform ADP of any Data Security Breach involving Personal Data. With regard to any such Data Security Breach, the Third Party Processor shall also take adequate remedial measures and provide ADP with all relevant information and assistance as may be reasonably requested by ADP);

(g) Upon termination of the agreement, the Third Party Processor shall, at the option of ADP, return the Personal Data and copies thereof to ADP or shall securely delete such Personal Data, except to the extent the agreement or Applicable Law provides otherwise.

If EEA Applicable Law so requires, the Processor Contract will also address the following:

(a) The Third Party Processor shall Process the Personal Data only in accordance with ADP's documented instructions, including on transfers of Personal Data to any Third Party Processor not covered by an Adequacy Decision, unless the Third Party Processor is required to do so under mandatory requirements applicable to the Third Party Processor and notified to ADP;

(b) The Third Party Processor shall impose confidentiality obligations on Staff with access to Personal Data;

(c) Other than as expressly needed to perform the services, the Third Party Processor shall only permit subcontractors to Process the Personal Data (i) with the prior written consent of ADP; and (ii) based on a validly entered into written or electronic agreement with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Third Party Processor under the Processor Contract and provided that the Third Party Processor remains liable to ADP for the performance of the subcontractor in accordance with the terms of the

Processor Contract. In case ADP provides generic consent for involvement of subcontractors, the Third Party Processors shall provide notice to ADP of any changes in its subcontractors and will provide ADP the opportunity to object to such changes based on reasonable grounds;

(d) The Third Party Processor shall deal promptly and appropriately with (i) requests for information necessary to demonstrate compliance of the Third Party Processor with its obligations under its Processor Contract and will inform ADP if any instructions of ADP in this respect violate EEA Applicable Law; (ii) requests and complaints of individuals as instructed by ADP; (iii) requests for assistance of ADP as reasonably required to ensure compliance of the Processing of the Personal Data with EEA Applicable Law; (iv) respond to any inquiries from ADP regarding its Processing activities;

Transfer of Data to Third Party not covered by an Adequacy Decision

11.6 This Article sets forth additional rules for the transfer of Personal Data that were collected in connection with the activities of a Group Company in countries that restrict cross-border transfers based on an assessment of the adequacy of the level of data protection in the recipient country. With regard to transfers of Personal Data subject to such transfer restrictions to a Third Party not covered by an Adequacy Decision, the Personal Data may only be transferred if:

(a) The transfer is necessary for (i) the performance of a contract (1) with the Individual, (2) with a Client, Supplier, or Business Partner for whom the Individual works, or (3) made in the interest of the Individual between ADP and the Third Party, or (ii) for contract execution and management (such as due diligence, negotiations, or other steps prior to contract execution);

(b) A contract has been concluded between ADP and the relevant Third Party (i) requiring that such Third Party shall be bound by the terms of this Code as if it was a Group Company, (ii) providing for a similar level of Personal Data protection as provided by this Code, or (iii) meeting applicable legal requirements for adequacy (*e.g.,* the contract conforms to any model contract requirement under Applicable Law);

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between ADP and a Third Party;

(d) The Third Party has been certified to a program that is recognized under Applicable Law as providing an adequate level of data protection;

(e) The Third Party has implemented Binding Corporate Rules or a similar transfer control mechanism which provides adequate safeguards under Applicable Law;

(f) The transfer is necessary to protect a vital interest of the Individual;

(g) The transfer is necessary for the establishment, exercise, or defense of a legal claim;

(h) The transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society;

(i) The transfer is necessary for the performance of a task carried out to comply with a legal obligation to which the relevant Group Company is subject; or

(j) The transfer is otherwise permissible under Applicable Law.

Items (h) and (i) above require the prior approval of the Global Data Privacy and Governance Team.

Consent for Transfer

11.7 If Applicable Law so requires, in addition to having one of the grounds listed in Article 11.6, ADP shall also seek consent for the relevant transfer.

If none of the grounds listed in Article 11.6 applies, ADP may request consent for transfer of the Personal Data. Prior to requesting consent, the Individual shall be provided with the information required for the consent to be deemed as informed consent, such as:

(a) The purpose of the transfer;

(b) The identity or categories of Third Parties to which the Data will be transferred;

(c) The categories of Data that will be transferred;

(d) Countries to which the Data will be transferred (and that the Data will be transferred to a Third Party not covered by an Adequacy Decision, if applicable); and

(e) Information about possible adverse consequences (if any) that may be foreseen as a result of the transfer.

Internal Processors

11.8 Internal Processors may Process Personal Data only if they have a validly entered into written or electronic contract with the Group Company being the Data Controller of the relevant Personal Data, which contract must in any event include the provisions set out in Article 11.5.

Article 12 – Overriding Interests

Overriding Interests

12.1 Some of the obligations of ADP or rights of Individuals under this Code may be overridden if, under specific circumstances, a pressing need exists that outweighs the interest of the Individual. An Overriding Interest exists if there is a need to:

(a) Protect the legitimate business interests of ADP including:

(1) The health, security, or safety of Staff, Client Employees, or other Individuals;

(2) ADP's intellectual property rights, trade secrets, or reputation;

(3) The continuity of ADP’s business operations;

(4) The preservation of confidentiality in a proposed sale, merger, or acquisition of a business; or

(5) The involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes;

(b) Prevent or investigate (including cooperating with law enforcement and Third Parties) suspected or actual violations of law; or

(c) Otherwise protect or defend the rights or freedoms of ADP, its Staff, Client Employees, or other Individuals.

Exceptions in the event of Overriding Interests

12.2 If an Overriding Interest exists, one or more of the following obligations of ADP or rights of the Individual may be set aside:

(a) Article 3.1 (the requirement to Process Personal Data for closely related purposes);

(b) Article 5.2 (data storage and deletion);

(c) Article 6.1 and 6.2 (information provided to Individuals, Personal Data not obtained from the Individuals);

(d) Article 7 (rights of Individuals);

(e) Articles 8.2 and 8.3 (Access limitations and confidentiality requirements); and

(f) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).

Special Categories of Data

12.3 The requirements of Articles 4.1, 4.2, and 4.3 (Special Categories of Data) may be set aside only for the Overriding Interests listed in Article 12.1 (a)(i)-(iii), (v), (b) and (c).

Consultation with the Global Data Privacy and Governance Team

12.4 Setting aside the obligations of ADP or rights of Individuals based on an Overriding Interest requires prior consultation with the Global Data Privacy and Governance Team, which shall document the advice given.

Information to Individual

12.5 Upon request of the Individual, ADP shall inform the Individual that an Overriding Interest exists for which the obligations of ADP or rights of the Individual have been set aside.

Article 13 – Supervision and Compliance

Global Chief Privacy Officer

13.1 The ADP Group shall have a Global Chief Privacy Officer who is responsible for:

(a) Chairing the Privacy Leadership Council;

(b) Supervising compliance with this Code;

(c) Supervising, coordinating, communicating, and consulting with the relevant members of the Privacy Network on privacy and data protection issues;

(d) Providing annual privacy reports on data protection risks and compliance issues to the ADP Executive Committee;

(e) Coordinating official investigations or inquiries into the Processing of Personal Data by a government authority, in conjunction with the relevant members of the Privacy Network and ADP's Legal department;

(f) Dealing with conflicts between this Code and Applicable Law;

(g) Approving data transfers as described in Articles 20.1 and 11.6;

(h) Monitoring the process by which Data Protection Impact Assessments are conducted and reviewing PIAs as appropriate;

(i) Monitoring the documentation, notification, and communication of Data Security Breaches;

(j) Resolving complaints as described in Article 17;

(k) Advising on the data management processes, systems, and tools to implement the framework for privacy and data protection management as established by the Privacy Leadership Council, including:

(1) Maintaining, updating, and publishing this Code and related policies and standards;

(2) Advising on the tools to collect, maintain, and update inventories containing information about the structure and functioning of all systems that Process Personal Data;

(3) Providing, assisting, or advising on the privacy training to Staff so that they understand and comply with their responsibilities under this Code;

(4) Coordinating with ADP's Internal Audit department and others to develop and maintain an appropriate assurance program to monitor, audit, and report compliance with this Code, and to enable ADP to verify and certify such compliance as needed;

(5) Implementing procedures as needed to address privacy and data protection inquiries, concerns, and complaints;

(6) Advising as to appropriate sanctions for violations of this Code (*e.g.*, disciplinary standards); and

(l) Other responsibilities as required by Applicable Law.

Privacy Network

13.2 ADP shall establish a Privacy Network sufficient to direct compliance with this Code within the ADP global organization.

The Privacy Network shall create and maintain a framework to support the Global Chief Privacy Officer and to undertake oversight of those tasks set forth in Article 13.1 and other tasks as may be appropriate to maintain and update this Code. The members of the Privacy Network shall perform, as relevant to their role in the region or organization, the following additional tasks:

(a) Oversee implementation of the data management processes, systems, and tools that enable adherence to the Code by the Group Companies in their respective regions or organizations;

(b) Support and assess overall privacy and data protection management and compliance of the Group Companies within their regions;

(c) Regularly advise Privacy Stewards and the Global Chief Privacy Officer on regional or local privacy risks and compliance issues;

(d) Verify that appropriate inventories of the systems that Process Personal Data are being maintained;

(e) Be available to respond to requests for privacy approvals or advice;

(f) Provide information needed by the Global Chief Privacy Officer to complete the annual privacy report;

(g) Assist the Global Chief Privacy Officer in the event of official investigations or inquiries by government authorities;

(h) Develop and publish privacy policies and standards appropriate for their regions or organizations;

(i) Advise Group Companies on data retention and destruction;

(j) Notify the Global Chief Privacy Officer of complaints and cooperate with the Global Data Privacy and Governance Team as described in Article 17; and

(k) Assist the Global Chief Privacy Officer, other members of the Privacy Network, Privacy Stewards and others as needed to:

(1) Enable the Group Companies or organizations to comply with the Code, using the instructions, tools, and trainings that have been developed;

(2) Share best practices for privacy and data protection management within the region;

(3) Confirm that privacy and data protection requirements are taken into account whenever new technology is implemented in the Group Companies or organizations; and

(4) Assist the Privacy Stewards, Group Companies, business units, functional areas, and procurement personnel with data transfers and the use of Third Parties and Subprocessors.

Privacy Stewards

13.3 Privacy Stewards are ADP executives who have been appointed by the Responsible Executives and/or ADP's Executive Leadership to implement and enforce the Codes within an ADP business unit or functional area. Privacy Stewards are accountable for effective implementation of the Code within the relevant business unit or functional area. In particular, Privacy Stewards must verify that effective privacy and data protection management controls are integrated into all business practices that impact Personal Data and that adequate resources and budget are available to meet the obligations

of the Codes. Privacy Stewards may delegate tasks and shall allocate appropriate resources, as needed, to meet their responsibilities and achieve compliance goals.

Privacy Stewards' responsibilities include:

(a) Monitoring overall privacy and data protection management and compliance within their Group Company, business unit, or functional area, and verifying that all processes, systems, and tools devised by the Global Data Privacy and Governance Team have been implemented effectively;

(b) Confirming that privacy and data protection management and compliance tasks are appropriately delegated in the normal course of business, as well as during and following organizational restructuring, outsourcing, mergers and acquisitions, and divestures;

(c) Collaborating with the Global Chief Privacy Officer and the relevant members of the Privacy Network to understand and address any new legal requirements, and verifying that the privacy and data protection management processes are updated to address changing circumstances and legal and regulatory requirements;

(d) Consulting with the Global Chief Privacy Officer and the relevant members of the Privacy Network in all cases where there is an actual or potential conflict between Applicable Law and this Code as described in Article 20.2;

(e) Monitoring Third Parties used by the Group Company, business unit, or functional area to confirm ongoing compliance by the Third Parties with this Code;

(f) Confirming that all Staff in the Group Company, business unit, or functional area have completed the required privacy training courses; and

(g) Directing that stored Personal Data be deleted, destroyed, de-identified, or transferred as required by Article 5.2.

Responsible Executives

13.4 The Responsible Executives, as heads of business units or functional areas, are responsible for ensuring that effective privacy and data protection management is implemented in their organizations. Each Responsible Executive shall (a) appoint appropriate Privacy Stewards, (b) ensure that adequate resources and budget are available for compliance, and (c) provide support to the Privacy Steward as needed to address compliance weaknesses and manage risk.

Privacy Leadership Council

13.5 The Global Chief Privacy Officer shall chair a Privacy Leadership Council comprised of the Privacy Stewards, members of the Privacy Network selected by the Global Chief Privacy Officer, and others who may be necessary to assist in the Council's mission. The Privacy Leadership Council shall create and maintain a framework to support the tasks as may be appropriate for the business units or functional areas to comply with this

Code, to undertake the tasks set forth herein, and to support the Global Chief Privacy Officer.

Default Privacy Network Members and Privacy Stewards 13.6 If at any time there is no Global Chief Privacy Officer appointed or in capacity to perform the functions assigned to the role, then the General Counsel shall appoint a person to act as interim Global Chief Privacy Officer. If at any time there is no member of the Privacy Network designated for a particular region or organization, the Global Chief Privacy Officer shall undertake the tasks of such member of the Privacy Network as set forth in Article 13.2.

If at any time there is no Privacy Steward designated for a Group Company, business unit, or functional area, the Responsible Executive shall appoint an appropriate person to undertake the tasks set forth in Article 13.3.

Statutory Positions 13.7 Where members of the Privacy Network, e.g., data protection officers under EEA Applicable Law, hold their positions pursuant to law, they shall carry out their job responsibilities to the extent they do not conflict with their statutory positions.

Article 14 – Policies and Procedures

Policies and Procedures 14.1 ADP shall develop and implement policies, standards, guidelines, and procedures to comply with this Code.

System Information 14.2 ADP shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Data, such as inventories of systems and processes that impact Personal Data, along with information generated in the course of Data Protection Impact Assessments. A copy of this information will be provided to the Lead DPA or to a DPA competent to audit under Article 16.2 upon request.

Data Protection Impact Assessment 14.3 ADP shall maintain a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used (Data Protection Impact Assessment). Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by ADP, the Processing still presents a residual high risk for the rights and freedoms of Customers, the Lead DPA will be consulted prior to such Processing taking place.

Article 15 – Training

Staff Training 15.1 ADP shall provide training on this Code and on related confidentiality and security obligations to all Staff who have access to Personal Data.

Article 16 – Monitoring and Auditing Compliance

Audits

16.1 ADP shall audit business processes and procedures that involve the Processing of Personal Data for compliance with this Code. In particular:

(a) The audits may be carried out in the course of the regular activities of ADP Internal Audit (including through the use of independent Third Parties), other internal teams engaged in assurance functions, and on an ad-hoc basis at the request of the Global Chief Privacy Officer;

(b) The Global Chief Privacy Officer may also request that an audit be conducted by an external auditor and will inform the Responsible Executive of the relevant business unit and/or the ADP Executive Committee as appropriate;

(c) Applicable professional standards of independence, integrity, and confidentiality shall be observed during the audit process;

(d) The Global Chief Privacy Officer and the appropriate member of the Privacy Network shall be informed of the results of the audits;

(e) To the extent that the audit reveals non-compliance with this Code, those findings will be reported to the applicable Privacy Stewards and Responsible Executives. The Privacy Stewards will cooperate with the Global Data Privacy and Governance Team to develop and execute an appropriate remediation plan;

(f) A copy of the audit results related to compliance with this Code will be provided to the competent DPA upon request.

DPA Audit

16.2 The Lead DPA is authorized to audit the facilities used by ADP for the Processing of Personal Data for compliance with this Code. In addition, a DPA competent pursuant to Article 18.2 will be authorized to audit the relevant data transfer for compliance with this Code.

DPA Audit Procedure

16.3 To facilitate any audit based on Article 16.2, the following procedure will be followed:

(a) Information sharing: ADP will attempt to resolve the request using alternative methods of providing information to the DPA including ADP audit reports, discussion with ADP subject matter experts, and review of security, privacy, and operational controls in place.

(b) Examinations: If the information available through these mechanisms is insufficient to address the DPA's stated objectives, ADP will provide the DPA with the opportunity to communicate with ADP's auditor and if required, a direct right to examine ADP's data processing facilities used to process the Personal Data on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of ADP.

This Article 16.3 supplements or clarifies the audit rights which DPAs may have under Applicable Law. In case of contradiction, the provisions of Applicable Law shall prevail.

Annual Report 16.4 The Global Chief Privacy Officer shall produce an annual report for the ADP Executive Committee on compliance with this Code, data protection risks, and other relevant issues. This report will reflect the information provided by the Privacy Network and others regarding local developments and specific issues within Group Companies.

Mitigation 16.5 ADP shall take appropriate steps to address any instances of non-compliance with this Code identified during compliance audits.

Article 17 – Complaints Procedure

Complaints 17.1 Individuals may file written complaints, including by electronic means, in respect of any claim they have under Article 18.1 or violations of their rights under Applicable Law. Each privacy statement shall include the procedure by which these complaints may be filed. Should any complaint be received through another channel it will be forwarded to the Global Data Privacy and Governance Team directly or via email to privacy@adp.com.

The Global Data Privacy and Governance Team shall be responsible for complaint handling. Each complaint will be assigned to an appropriate Staff member (either within the Global Data Privacy and Governance Team or within the applicable business unit or functional area). These Staff will:

(a) Promptly acknowledge receipt of the complaint;

(b) Analyze the complaint and, if needed, initiate an investigation;

(c) If the complaint is well-founded, advise the applicable Privacy Steward and the relevant member of the Privacy Network so that a remediation plan can be developed and executed; and

(d) Maintain records of all complaints received, responses given, and remedial actions taken by ADP.

Reply to Individual 17.2 ADP will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Individual within four weeks of the date the complaint was filed. The response will be in writing and will be sent to the Individual via the means that the Individual originally used to contact ADP (*e.g.*, via mail or email). The response will outline the steps that ADP has taken to investigate the complaint and will indicate ADP's decision regarding what steps (if any) it will take as a result of the complaint.

In the event that ADP cannot reasonably complete its investigation and response within four weeks, it shall inform the Individual within eight weeks that the investigation is ongoing and that a response will be provided within the next four week period.

Complaints Privacy Network 17.3 An Individual may file a written complaint, including by electronic means, directly with designated members of the Privacy Network or with the Global Chief Privacy Officer if:

(a) The resolution of the complaint by the Global Data Privacy and Governance Team is unsatisfactory to the Individual (*e.g.*, the complaint is rejected);

(b) The Individual has not received a response as required by Article 17.2;

(c) The time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or

(d) The complaint stems from the Individual's attempt to exercise the rights set forth in Article 7, as described in Article 7.4.

Upon receipt of a direct complaint, the relevant member of the Privacy Network or the Global Chief Privacy Officer (as applicable) shall acknowledge the complaint and conduct an appropriate investigation. The procedures described in Article 17.2 shall apply to complaints filed with the designated members of the Privacy Network or the Global Chief Privacy Officer under this Article.

If the response of the designated member of the Privacy Network or the Global Chief Privacy Officer to the complaint is unsatisfactory to the Individual (e.g., the request is denied), the Individual can file a complaint or claim with the authorities or the courts in accordance with Article 18.2.

Article 18 – Legal Issues

Rights of Individuals

18.1 If ADP violates this Code with respect to the Personal Data of an Individual (**Affected Individual**) covered by this Code, the Affected Individual can as a third party beneficiary enforce any claim as a result of a breach of Articles 1.6, 2 – 11, 12.5, 16.2, 17, 18 and 20.4 – 20.5 in accordance with Article 18.2.

The rights contained in this Article are in addition to, and shall not prejudice, any other rights or remedies that an Individual may otherwise have by law.

Local Law and Jurisdiction

18.2 Individuals are encouraged to first follow the complaints procedure set forth in Article 17 of this Code before filing any complaint or claim with the authorities or the courts.

In case of a violation of this Code, the Individual may, at his or her choice, submit a complaint or a claim to the DPA or the courts:

(a) in the EEA country at the origin of the data transfer, against the Group Company being the Data Controller responsible for the relevant data transfer;

(b) in the Netherlands, against the ADP Delegated Entity; or

(c) in the EEA country where (a) the Individual has his or her habitual residence or place of work; or (b) the infringement took place, against the Group Company being the Data Controller of the relevant Data.

The Group Company against which the complaint or claim is brought (relevant Group Company), may not rely on a breach by another Group Company or a Third Party Processor to avoid liability except to the extent any defense of such other Group Company or Third Party Processor would also constitute a defense of the relevant Group Company.

The DPAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Individual will not prejudice the substantive or procedural rights he or she may have under applicable law.

Right to claim damages

18.3 In case an Individual has a claim under Article 18.2, such Individual shall be entitled to compensation of any damages to the extent provided by applicable EEA law, suffered as a result of a violation of this Code.

Burden of proof in respect of claim for damages

18.4 In case an Individual brings a claim for damages under Article 18.2, it will be for the Individual to demonstrate that he or she has suffered damages and to establish facts which show it is plausible that the damage has occurred because of a violation of this Code. It will subsequently be for the relevant Group Company to prove that the damages suffered by the Individual due to a violation of this Code are not attributable to ADP.

Mutual assistance and redress

18.5 All Group Companies shall co-operate and assist to the extent reasonably possible with:

(a) handling requests, complaints, or claims made by an Individual; or

(b) complying with a lawful investigation or inquiry by a competent DPA or government authority.

The Group Company that receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his or her request, complaint, or claim except where circumstances dictate otherwise.

Advice of the Competent DPA

18.6 ADP shall, in good faith, cooperate with and use all reasonable efforts to follow the advice of the Lead DPA and the competent DPA under Article 18.2 issued on the interpretation and application of this Code. ADP shall abide by binding decisions of competent DPAs.

Mitigation

18.7 The ADP Delegated Entity shall ensure that adequate steps are taken to address violations of this Code by a Group Company.

Law applicable to this Code

18.8 This Code shall be governed by and interpreted in accordance with Dutch law.

Article 19 – Sanctions for Non-compliance

Non-compliance	19.1	Non-compliance of Staff with this Code may result in appropriate disciplinary measures in accordance with Applicable Law and ADP policies, up to and including termination of the employment relationship or contract.

Article 20 – Conflicts between this Code and Applicable Law

Conflict of Law when Transferring Data from the EEA	20.1	Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA, the transfer requires the prior approval of the Global Data Privacy and Governance Team. The privacy officer for Europe and/or the Global Chief Privacy Officer may also consult with the Lead DPA or another competent government authority.
Conflict between Code and Law	20.2	In all other cases, where there is a conflict between Applicable Law and this Code, the Responsible Executive, or the Privacy Steward shall consult with the Global Chief Privacy Officer, the relevant member(s) of the Privacy Network (as appropriate), and the business unit's Legal department to determine how to comply with this Code, and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to ADP.
New Conflicting Legal Requirements	20.3	Members of the Legal department, ADP Business Security Officers, and Privacy Stewards shall promptly inform the Global Data Privacy and Governance Team of any new legal requirements which they become aware of that may interfere with ADP's ability to comply with this Code. The relevant Privacy Stewards, in consultation with the Legal department, shall promptly inform the Responsible Executive of any new legal requirement that may interfere with ADP's ability to comply with this Code.
Reporting to Lead DPA	20.4	If ADP becomes aware that applicable local law of a non-EEA country is likely to have a substantial adverse effect on the protection offered by this Code, ADP will report this to the Lead DPA.
Requests for Disclosure of Personal Data	20.5	If ADP receives a request for disclosure of Personal Data from a law enforcement authority or state security body of a non-EEA country (**Authority**), it will first assess on a case-by-case basis whether this request (**Disclosure Request**) is legally valid and binding on ADP. Any Disclosure Request that is not legally valid and binding on Company will be resisted in accordance with applicable law. Subject to the following paragraph, ADP shall promptly inform the Lead DPA of any legally valid and binding Disclosure Requests, and will request the Authority to put such Disclosure Requests on hold for a reasonable delay in order to enable the Lead DPA to issue an opinion on the validity of the relevant disclosure.

If suspension and/or notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, ADP will request the Authority to waive this prohibition and will document that it has made this request. In any event, ADP will on an annual basis provide to the Lead DPA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by applicable law.

Any transfers by ADP of Personal Data to any Authority in response to a Disclosure Request will not be massive, disproportionate or indiscriminate.

Article 21 – Changes to this Code

Approval for Changes 21.1 Any material changes to this Code require the prior approval of the Global Chief Privacy Officer and the General Counsel, as well as adoption by the ADP Executive Committee and shall thereafter be communicated to Group Companies**.** The ADP Delegated Entity shall promptly inform the Lead DPA of changes to this Code that have a significant impact on the protection offered by this Code or the Code itself and will be responsible for coordinating ADP's responses to questions of the Lead DPA in respect hereof. The Global Chief Privacy Officer shall inform the appropriate Privacy Stewarts of the effect of such responses. Other changes (if any) will be notified by the Chief Privacy Officer to the Lead DPA on a yearly basis.

Consent Not Required for Non-material Changes 21.2 ADP shall not be required to obtain consent from Individuals prior to making changes to this Code, provided that the changes do not have a material and adverse impact on the Individuals, such as changes that confer additional rights or benefits on the Individuals.

Effective Date of Changes 21.3 Any change shall enter into force with immediate effect after it has been approved in accordance with Article 21 and published on the www.adp.com website.

Prior Versions 21.4 Any request, complaint, or claim of an Individual involving this Code shall be judged against the version of this Code as it is in force at the time the request, complaint, or claim is made.

Article 22 – Implementation and Transition Periods

Implementation 22.1 The implementation of this Code shall be supervised by Privacy Stewards, with the assistance of the Global Data Privacy and Governance Team. Except as indicated below, there shall be an eighteen-month transition period from the Effective Date (as set forth in Article 1.7) for compliance with this Code.

Accordingly, except as otherwise indicated, within eighteen months of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with this Code, and the Code shall be fully in force. During the transition period, the Code shall become effective for a Group Company, as soon as such Group Company completes the tasks necessary for full implementation and such Group Company has provided appropriate notice to the Global Chief Privacy Officer.

This Code may be used as a data transfer mechanism by the applicable Group Companies, business units, and functional areas after the Effective Date, subject to any prior authorization requirements that may exist under Applicable Law. To the extent that a Group Company, business unit or functional area receiving such Personal Data has not also implemented this Code, the data transfer must meet one of the grounds for transfer listed in Articles 11.6 – 11.7.

New Group Companies 22.2 Any entity that becomes a Group Company after the Effective Date shall comply with this Code within two years of becoming a Group Company.

Divested Entities 22.3 A Divested Entity (or specific parts thereof) may remain covered by this Code after its divestment for such period as may be required by ADP to disentangle the Processing of Personal Data related to such Divested Entity.

Transition Period for Existing Agreements 22.4 Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business provided, however, that all such existing agreements shall be in compliance with this Code within eighteen months of the Effective Date.

Transitional Period for Local-for-Local Processing 22.5 Local-for-Local Processing subject to this Code shall be brought into compliance with this Code within five years of the Effective Date.

Contact Details ADP Global Data Privacy and Governance Team: privacy@adp.com

ADP Delegated Entity
ADP Nederland B.V.
Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
THE NETHERLANDS

Interpretations INTERPRETATION OF THIS CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;

(ii) Headings are included for convenience only and are not to be used in construing any provision of this Code;

(iii) If a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(iv) The male form shall include the female form;

(v) The words "include," "includes," "including," and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;

(vi) The word “written” shall include any documented communication, writing, contract, electronic record, electronic signature, facsimile copy, or other legally valid and enforceable instrument without regard to format;

(vii) A reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented, or replaced, except to the extent prohibited by this Code or the referenced document; and

(viii) A reference to law includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

Annex 1 – BCR Definitions

Adequacy Decision	ADEQUACY DECISION means any determination by a Data Protection Authority, or other competent body, that a country, a region or a recipient of a data transfer is deemed to provide an adequate level of protection for the Personal Data. Entities covered by an Adequacy Decision include recipients located in countries that under Applicable Law are deemed to provide an adequate level of data protection as well as recipients who are bound by another instrument (such as a set of Binding Corporate Rules) that have been approved by the applicable Data Protection Authority or other competent body. With regard to the United States, companies that become certified to any US-EEA and/or US-Swiss privacy framework would be covered by an Adequacy Decision.
ADP (ADP Group)	ADP (the ADP GROUP) means, collectively, Automatic Data Processing, Inc. (the Parent Company) and the Group Companies, including ADP, Inc.
ADP Contracting Entity	ADP CONTRACTING ENTITY means the Group Company that has entered into a contract required by the Codes, such as a Service Contract, Subprocessor Contract, or data transfer agreement.
ADP Delegated Entity	ADP DELEGATED ENTITY means ADP Nederland, B.V., having its registered seat in Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, the Netherlands.
ADP Executive Committee	ADP EXECUTIVE COMMITTEE means the committee of officers consisting of (i) Automatic Data Processing, Inc.'s chief executive officer (CEO), and (ii) those other officers that report directly to the CEO and that, collectively, have responsibility for the ADP group operations.
ADP Subprocessor	For the purpose of the Privacy Code for Client Data Processing Services, an ADP SUBPROCESSOR means any Group Company engaged by another Group Company as a Subprocessor for Client Data.
Applicable Data Controller Law	For the purpose of the Privacy Code for Client Data Processing Services, APPLICABLE DATA CONTROLLER LAW means any privacy or data protection laws that apply to an ADP Client as the Data Controller of such Client Data.
Applicable Data Processor Law	For the purpose of the Privacy Code for Client Data Processing Services, APPLICABLE DATA PROCESSOR LAW means any privacy or data protection laws that apply to ADP as a Data Processor, on behalf of a Client who is a Data Controller.
Applicable Law	APPLICABLE LAW means any privacy or data protection laws that are applicable to any particular Processing activities.
Applicant	APPLICANT means any Individual who provides Personal Data to ADP in the context of applying for a position with ADP as an Associate.

Archive	ARCHIVE means a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data were originally collected, or that are no longer used for general business activities but are potentially used only for historical, scientific, or statistical purposes, dispute resolution, investigations, or general archiving purposes. Access to an Archive is limited to system administrators and others whose jobs specifically require access to the archive.
Associate	ASSOCIATE means an Applicant, a current ADP employee, or a former ADP employee, with the exception of a Co-Employed Individuals. NOTE: the ADP Workplace Privacy Code therefore does not apply to the Processing of Personal Data of Co-Employed Individuals.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. is the parent company of the ADP Group, and is a Delaware (USA) corporation having its principal place of business at One ADP Boulevard, Roseland, New Jersey, 07068-1728, USA.
Binding Corporate Rules	BINDING CORPORATE RULES means a privacy policy of a group of related companies considered to provide an adequate level of protection for the transfer of Personal Data within that group of companies under Applicable Law.
Business Contact Data	BUSINESS CONTACT DATA means any data pertaining to a Professional typically found on a business card or in an email signature.
Business Partner	BUSINESS PARTNER means any Third Party, other than a Client or Supplier that has, or had a business relationship or strategic alliance with ADP (*e.g.*, joint marketing partner, joint venture, or joint development partner).
Business Purpose	BUSINESS PURPOSE means a legitimate purpose for Processing Personal Data as specified in Article 2, 3 or 4 of any ADP Code, or for Processing Special Categories of Data as specified in Article 4 of any ADP Code.
Children	For purposes of ADP's data collection and marketing, CHILDREN means Individuals under the age determined by applicable law as able to consent to such data collection and/or marketing.
Client	CLIENT means any Third Party that utilizes one or more ADP products or services in the course of its own business.
Client Data	CLIENT DATA means Personal Data pertaining to Client Employees (including prospective employees, past employees, and dependents of employees) Processed by ADP in connection with providing Client Services.

Client Employee	CLIENT EMPLOYEE means any Individual whose Personal Data are Processed by ADP as a Data Processor for a Client pursuant to a Services Agreement. For the sake of clarity, CLIENT EMPLOYEE refers to all Individuals whose Personal Data are Processed by ADP in performing Client Services (regardless of the legal nature of the relationship between the Individual and the Client). It does not include Professionals whose Personal Data are Processed by ADP in connection with ADP's direct relationship with the Client. For example, ADP may Process Personal Data of an HR Professional in order to enter into a contract with the Client--this Data are subject to the Privacy Code for Business Data. However, when ADP provides payroll Processing services to the Client (e.g., issues pay slips, provides assistance on the use of an ADP system), the Individual's data would be Processed as Client Data.
Client Services	CLIENT SERVICES means the human capital management services provided by ADP to Clients, such as recruiting, payroll and compensation services, employee benefits, talent management, HR administration, consulting and analytics, and retirement services.
Client Support Activities	CLIENT SUPPORT ACTIVITIES means those Processing activities undertaken by ADP to support the delivery of its products and services. Client Support Activities may include, for example, training Professionals, responding to questions about the services, opening and resolving support tickets, providing product and service information (including updates and compliance alerts), quality control and monitoring, and related activities that facilitate effective use of ADP's products and services.
Code	CODE means (as applicable) the ADP Privacy Code for Business Data, the ADP Workplace Privacy Code (internal to ADP), and the ADP Privacy Code for Client Data Processing Services; collectively referred to as the Codes.
Co-Employed Individual	CO-EMPLOYED INDIVIDUAL means an employee of a U.S. Client who is co-employed by an indirect US affiliate of Automatic Data Processing, Inc. as part of the professional employer organization service offering in the U.S.
Consumer	CONSUMER means an Individual who interacts directly with ADP in a personal capacity. For example, Consumers include individuals who participate in talent development programs or utilize products and services from ADP for their personal use (*i.e.*, outside of an employment relationship with ADP or an ADP Client).
Contingent Worker	CONTINGENT WORKER means an Individual who provides services to ADP (and who are subject to ADP's direct supervision) on a provisional or non-permanent basis, such as temporary workers, contract workers, independent contractors, or consultants.
Data Controller	DATA CONTROLLER means the entity or natural person which alone, or jointly with others, determines the purposes and means of the Processing of Personal Data.

Data Processor	DATA PROCESSOR means the entity or natural person which Processes Personal Data on behalf of a Data Controller.
Data Protection Authority or DPA	DATA PROTECTION AUTHORITY OR DPA means any regulatory or supervisory authority that oversees data protection or privacy in a country in which a Group Company is established.
Data Protection Impact Assessment (DPIA)	DATA PROTECTION IMPACT ASSESSMENT (DPIA) shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain: (i) a description of: (a) the scope and context of the Processing; (b) the Business Purposes for which Personal Data are Processed; (c) the specific purposes for which Special Categories of Data are Processed; (d) categories of Personal Data recipients, including recipients not covered by an Adequacy Decision; (e) Personal Data storage periods; (ii) an assessment of: (a) the necessity and proportionality of the Processing; (b) the risks to the privacy rights of Individuals; and the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Data.
Data Security Breach	DATA SECURITY BREACH means any incident that impacts the confidentiality, integrity, or availability of Personal Data, such as unauthorized use or disclosure of Personal Data, or unauthorized access to Personal Data, that compromises the privacy or security of the Personal Data.
Dependent	DEPENDENT means the spouse, partner, child, or beneficiary of an Associate, or the emergency contact of an Associate or Contingent Worker.
Divested Entity	DIVESTED ENTITY means a Group Company that is no longer owned by ADP as a result of the sale of company shares and/or assets, or other divestiture, so that the company no longer qualifies as a Group Company.

EEA	EEA or EUROPEAN ECONOMIC AREA means all Member States of the European Union, plus Norway, Iceland, and Liechtenstein and for purposes of the Codes, Switzerland and the United Kingdom (UK) after its exit from the European Union. By decision of the General Counsel – to be published on www.adp.com it may include other countries with data protection laws having data transfer restrictions similar to EEA Data Transfer Restrictions.
EEA Applicable Law	EEA APPLICABLE LAW means the requirements under the Applicable Laws of the EEA, which are applicable to any Personal Data that are originally collected in the context of the activities of a Group Company established in the EEA (also after being transferred to another Group Company established outside the EEA).
EEA Data Transfer Restriction	EEA DATA TRANSFER RESTRICTION means any restriction regarding cross-border transfers of Personal Data under the data protection laws of a country of the EEA.
Effective Date	EFFECTIVE DATE means the date on which the Codes become effective as set out in Article 1 of the Codes.
General Counsel	GENERAL COUNSEL means the General Counsel of Automatic Data Processing, Inc.
Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER means the ADP Associate who holds this title at Automatic Data Processing, Inc.
Group Company	GROUP COMPANY means any legal entity that is an affiliate of Automatic Data Processing, Inc. and/or ADP, Inc., if either Automatic Data Processing, Inc. or ADP, Inc. directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such legal entity.
Individual	INDIVIDUAL means any identified or identifiable natural person whose Personal Data are Processed by ADP either as a Data Processor or a Data Controller, with the exception of Co-Employed Individuals. NOTE: the ADP Privacy Code for Business Data and the ADP Workplace Privacy Code therefore do not apply to the Processing of Personal Data of Co-Employed Individuals.
Internal Processor	INTERNAL PROCESSOR shall mean any Group Company that Processes Personal Data on behalf of another Group Company being the Data Controller.
Lead DPA	LEAD DPA shall mean the Dutch Data Protection Authority.

Mandatory Requirements	MANDATORY REQUIREMENTS shall mean those obligations under any Applicable Data Processor Law which require Processing of Personal Data for (i) national security or defense; (ii) public safety; (iii) the prevention, investigation, detection, or prosecution of criminal offences or of breaches of ethics for regulated professions; or (iv) the protection of any Individual, or the rights and freedoms of Individuals.
Global Data Privacy and Governance Team	GLOBAL DATA PRIVACY & GOVERNANCE TEAM means ADP's Office of Privacy and Data Governance. The Office of Privacy and Data Governance is led by the Global Chief Privacy Officer and consists of privacy officers, privacy managers and other Staff with reporting relationships to the Global Chief Privacy Officer or the privacy officers and privacy managers.
Overriding Interest	OVERRIDING INTEREST means the pressing interests set forth in Article 13.1 of the ADP Workplace Privacy Code and the ADP Privacy Code for Business Data based on which the obligations of ADP or rights of Individuals set forth in Article 13.2 and 13.3 of the Codes may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.
Personal Data or Data	PERSONAL DATA or DATA means any information relating to an identified or identifiable Individual. Personal Data may also be referred to as personal information in policies and standards that implement the Codes.
Privacy Leadership Council	PRIVACY LEADERSHIP COUNCIL means the council led by the Global Chief Privacy Officer and comprised of the Privacy Stewards, members of the Privacy Network selected by the Global Chief Privacy Officer, and others who may be necessary to assist in the Council's mission.
Privacy Network	PRIVACY NETWORK means the members of the Global 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.
Privacy Steward	PRIVACY STEWARD means an ADP executive who has been appointed by a Responsible Executive and/or ADP's Executive Leadership to implement and enforce the Privacy Codes within an ADP Business Unit.
Processing	PROCESSING means any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission, or deletion of Personal Data.
Processor Contract	PROCESSOR CONTRACT shall mean any contract for the Processing of Personal Data entered into by ADP and a Third Party Processor.
Professional	PROFESSIONAL means any individual (other than an employee) who interacts directly with ADP in a professional or business capacity. For

	example, Professionals include Client HR staff who engage with ADP as users of ADP's products or services. Professionals also include Client, Supplier, and Business Partner account representatives, business contacts, trade association contacts, regulators, media contacts, and other individuals who interact with ADP in a commercial capacity.
Responsible Executive	RESPONSIBLE EXECUTIVE means the Managing Director of a Group Company, or head of a business unit or functional area, who has primary budgetary ownership for the Group Company, business unit, or functional area.
Secondary Purpose	SECONDARY PURPOSE means any purpose other than the Original Purpose for which Personal Data are further Processed.
Service Agreement	SERVICE AGREEMENT means any contract, agreement, or terms pursuant to which ADP provides Client Services to a Client.
Special Categories of Data	SPECIAL CATEGORIES OF DATA means Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, or proceedings with regard to criminal or unlawful behavior.
Staff	STAFF means, collectively, currently-employed ADP Associates and those Contingent Workers who are currently working for ADP.
Subprocessor Contract	SUBPROCESSOR CONTRACT means a written or electronic agreement between ADP and a Third Party Subprocessor pursuant to Article 7.1 of the Privacy Code for Client Data Processing Services.
Subprocessors	SUBPROCESSORS means, collectively, ADP Subprocessors and Third Party Subprocessors.
Supplier	SUPPLIER means any Third Party that provides goods or services to ADP (e.g., as a service provider, agent, Data Processor, consultant or vendor).
Third Party	THIRD PARTY means any person, private organization, or government body that is not a Group Company.
Third Party Controller	THIRD PARTY CONTROLLER means a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR means a Third Party that Processes Personal Data on behalf of ADP that is not under the direct authority of ADP.
Third Party Subprocessor	THIRD PARTY SUBPROCESSOR means any Third Party engaged by ADP as a Subprocessor.

Annex 2 – List of Group Companies bound by the ADP Privacy Code for Business Data

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Philippines, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Switzerland
ADP Aviation, LLC	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Benefit Services KY, Inc.	11405 Bluegrass Parkway Louisville, KY, USA 40299
ADP Brasil Ltda	Rua João Tibiriçá, n.º 1112 – Vila Anastácio – São Paulo/SP. 05077-000
ADP Broker-Dealer, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Credit Corp.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Brussels, Belgium
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, Czech Republic
ADP Employer Services CIS	Varshavskoe shosse 125, 117545 Moscow, Russian Federation
ADP Employer Services Denmark ApS	c/o Intertrust A/S, Harbour House, Sundkrogsgade 21, 2100 Copenhagen, Denmark
ADP Employer Services GmbH-2	Frankfurter Str. 227, 63263 Neu-Isenburg, Germany
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, Spain
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milan, Italy
ADP Employer Services Mexico, S.A. de C.V.	Medanos No. 169, Colonia Las Aguilas, C.P. 01710, Alvaro Obregon, Distrito Federal, Mexico
ADP Employer Services Sweden AB	c/o Intertrust Sweden AB, Strandvägen 7 A, 114 56 Stockholm, Sweden
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunis, Tunisia

ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, France
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Netherlands
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, France
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP Human Resources Service Company Limited	Unit 738, 7/F., Low Block, Grand Millennium Plaza, 181 Queen's Road Central, Hong Kong
ADP Human Resources Services (Shanghai) Co., Ltd.	5F, Building 2, YouYou Century Place, 428 Yanggao Road South, Shanghai 200127, The People's Republic of China
ADP Indemnity, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 India
ADP International Services BV	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Netherlands
ADP MasterTax, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam
ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milan, Italy
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Warsaw, Poland
ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, India – 500082
ADP Residential Real Estate Services, LLC	One ADP Boulevard, Roseland, NJ, USA 07068
ADP RPO Japan G.K.	7th Floor, Toanomon 40 MT Building, 5-13-1 Toranomon, Minato-ku, Tokyo, Japan
ADP RPO Singapore Pte Limit	28 Bukit Pasoh Road, Yee Lan Court, Singapore, 089842

ADP RPO UK Limited	22 Chancery Lane, London, England, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovakia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turin, Italy
ADP Strategic Plan Services, LLC	71 Hanover Road, Mail Stop 580, Florham Park, NJ, USA 07932
ADP Tax Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP TotalSource CO XXI, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource CO XXII, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource DE IV, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XI, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XIX, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XVI, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XVII, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XVIII, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource FL XXIX, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource Group, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource I, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource II, Inc.	10200 Sunset Drive, Miami, FL, USA 33173

ADP TotalSource III, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI V, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI VI, LLC	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI VII, LLC	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI XXV, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI XXVI, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource MI XXX, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource NH XXVIII, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource of CO XXIII, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource Services, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP TotalSource, Inc.	10200 Sunset Drive, Miami, FL, USA 33173
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucharest, Romania 020334
Automatic Data Processing Insurance Agency, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing Limited	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (Hong Kong)	36/F. Tower Two, 1 Matheson Street, Causeway Bay, Hong Kong
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT
Automatic Data Processing Pte. Ltd.	78 Shenton Way, #26-01, Singapore 079120
Automatic Data Processing, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068

Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62 Ubi Road 1, #11-07 Oxley Bizhub 2 Singapore 408734
Celergo UK Limited	1 Fetter Lane, London, EC4A 1BR
Federal Liaison Services LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Global Cash Card, Inc.	7 Corporate Park, Suite 130, Irvine, California, USA 92606
MasterTax Service, LLC	7150 e. Camelback Road, Suite 10, Scottsdale, AZ, USA 85251
MasterTax, LLC	7150 e. Camelback Road, Suite 10, Scottsdale, AZ, USA 85251
OnForce Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
OnForce, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Payroll Peru SAC	Av. Alfredo Benavides 768 oficina 1202, Miraflores, Lima, Peru
Payroll S.A.	Av. Apoquindo 5400, piso 16, comuna de Las Condes, Santiago de Chile
Resources Enterprise Services - Workers Compensation LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Resources Enterprise Services LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068
W. Ray Wallace & Associates, Inc.	11700 Great Oaks Way, Suite 200, Alpharetta, GA, USA 30022

Work Market, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068