ADP Privacy Code for Client Data Processing Services

Introduction	2
Article 1 – Scope, Applicability and Implementation	2
Article 2 – Service Agreement	3
Article 3 – Compliance Obligations	4
Article 4 – Data Processing Purposes	6
Article 5 – Security Requirements	7
Article 6 – Transparency to Client Employees	7
Article 7 – Subprocessors	8
Article 8 – Supervision and Compliance	8
Article 9 – Policies and Procedures	12
Article 10 – Training	12
Article 11 – Monitoring and Auditing Compliance	12
Article 12 – Legal Issues	15
Article 13 – Sanctions for Non-compliance	18
Article 14 – Conflicts between this Code and Applicable Data Processor Law	18
Article 15 – Changes to this Code	19
Article 16 – Implementation and Transition Periods	19
ANNEX 1 – BCR Definitions	22
ANNEX 2 – Security Measures	30
ANNEX 3 – List of Group Companies bound by Processor Code	60

ADP Privacy Code for Client Data Processing Services

Introduction

ADP provides a wide range of human capital management services to its Clients. ADP has committed itself to the protection of Personal Data in the **ADP Code of Business Conduct and Ethics.**

This ADP Privacy Code for Client Data Processing Services indicates how this commitment is implemented for the Processing of Personal Data pertaining to Client Employees by ADP, in connection with providing Client Services and Client Support Activities. In this framework, Client Data is Processed by ADP as Data Processor on behalf of its Clients.

For the rules applicable to ADP's Processing of Personal Data as a Data Controller pertaining to those Individuals with whom ADP has a business relationship (e.g., Individuals who represent ADP's Clients, Suppliers, Business Partners, other Professionals, and Consumers) and other Individuals whose Personal Data is processed by ADP in the context of its business activities as a Data Controller, refer to the ***ADP Privacy Code for Business Data***.

Article 1 – Scope, Applicability and Implementation

Scope – Applicability to EEA Data

1.1 This Code addresses the Processing of Personal Data of Client Employees by ADP in its role as a Data Processor for Clients in the course of delivering Client Services, where such Personal Data are (a) subject to EEA Applicable Law (or were subject to EEA Applicable Law prior to the transfer of such Personal Data to a Group Company outside the EEA in a country which has not been deemed to provide an adequate level of data protection by competent EEA institutions);; and (b) Processed pursuant to a Service Agreement that specifically provides that this Code shall apply to such Personal Data.

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.

Electronic and Paper-based Processing

1.2 This Code applies to the Processing of Client Data by ADP by electronic means and in systematically accessible paper-based filing systems.

Applicability of Local Law

1.3 Nothing in this Code shall be construed to take away any rights or remedies that Client Employees 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 provides additional safeguards, rights, or remedies for Individuals, this Code shall apply.

Policies and Guidelines **1.4** ADP may supplement this Code through policies, standards, guidelines, and instructions that are consistent with this Code.

Accountability **1.5** 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 **1.6** 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. This Code will enter into force as of 11 April 2018 (**Effective Date**). The Code (including a list of the Group Companies involved in Processing of Client Data) 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 16.

Prior Policies **1.7** 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 **1.8** Automatic Data Processing, Inc. has appointed ADP Nederland B.V., having its registered seat in Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, The Netherlands, as the ADP Delegated Entity, in charge of enforcing this Code within the ADP Group, and ADP Nederland B.V., has accepted this appointment.

Article 2 – Service Agreement

Service Agreement, Subprocessors **2.1** ADP shall Process Client Data only on the basis of a Service Agreement which incorporates the mandatory data processor contracting requirements under Applicable Data Processor Law and for the Legitimate Purposes specified in Article 4.
The ADP Contracting Entity uses Subprocessors, both ADP Subprocessors and Third Party Subprocessors, in the regular performance of Client Services. ADP's Service Agreements shall authorize the use of such Subprocessors, provided that the ADP Contracting Entity remains liable to the Client for the performance by the Subprocessors in accordance with the terms of the Service Agreement. The provisions of Article 7 shall further govern the use of Subprocessors.

Termination of the Service Agreement

2.2 Upon termination of the Client Services, ADP shall fulfill its obligations to the Client in the Service Agreement with regard to the return of Client Data by providing to the Client the Client Data required for the continuity of the business activities of the Client (if the data has not been previously provided or made accessible to the Client via relevant product functionality, such as the ability to download the Client Data).

When ADP's obligations under the Service Agreement have been fulfilled, ADP shall securely destroy remaining copies of the Client Data, and (upon request of the Client) certify to the Client that it has done so. ADP may maintain a copy of Client Data to the extent required under Applicable Law, as authorized by the Client, or as needed for dispute resolution purposes. ADP shall no longer Process that Client Data, except to the extent required for the aforementioned purposes. ADP's obligations of confidentiality under the related Service Agreement will persist for as long as ADP maintains a copy of such Client Data.

Audit of Termination Measures

2.3 Within 30 days after termination of the Service Agreement (unless required otherwise by a competent Data Protection Authority), ADP shall, at the request of the Client or of the competent Data Protection Authority, allow its Processing facilities to be audited in accordance with Articles 11.2 or 11.3 (as applicable) to verify that ADP complies with its termination-related obligations under Article 2.2.

Article 3 – Compliance Obligations

Instructions of the Client

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

Compliance with Applicable Law

3.2 ADP shall Process Client Data in accordance with the Applicable Data Processor Law.

ADP shall respond promptly and appropriately to requests for assistance from the Client, as legally required, to enable the Client to comply with its obligations under the Applicable Data Controller Law, in accordance with the Service Agreement.

Non-compliance, Substantial Adverse Effect

3.3 If a Group Company becomes aware that Applicable Data Processor Law of a non-EEA country, or any change in Applicable Data Processor Law of a non-EEA country, or an instruction of the Client, is likely to have a substantial adverse effect on ADP's ability to meet its obligations under 3.1, 3.2 or 11.3, such Group Company shall promptly notify the ADP Delegated Entity and the Client thereof,

in which case the Client will have the right under this Code to temporarily suspend the relevant transfer to ADP of Client Data, until such time as the Processing is adjusted to remedy the non-compliance. In the event that an adjustment is not possible, the Client shall have the right to terminate the relevant part of the Processing by ADP, in accordance with the terms of the Service Agreement. These rights and obligations do not apply when the circumstances or change in Applicable Data Processor Law result from Mandatory Requirements.

Request for Disclosure of Client Data

3.4 If ADP receives a request for disclosure of Client 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 is legally valid and binding on ADP. Any request that is not legally valid and binding on ADP will be resisted in accordance with Applicable Law.

Subject to the following paragraph, ADP shall promptly inform the Client, the Lead DPA and the DPA competent for the Client under Article 11.3 of any such Authority request which is legally valid and binding on ADP, and will request the Authority to put it on hold for a reasonable period, in order to enable the Lead DPA to issue an opinion regarding the validity of the requested disclosure.

If the suspension of the enforcement and/or notification to the Lead DPA of a legally valid and binding disclosure request is prohibited, such as in the 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. ADP will provide general information on the number and type of disclosure requests it received in the preceding 12-month period from Authorities to the Lead DPA on an annual basis.

This Article does not apply to requests received by ADP from authorities in the normal course of its activities as an HCM services provider (such as court orders to garnish wages), which ADP can continue to provide in accordance with Applicable Law, the Service Agreement and Clients' instructions.

Client Inquiries

3.5 ADP shall respond promptly and appropriately to Client inquiries related to the Processing of the Client Data pursuant to the terms of the Service Agreement.

Article 4 – Data Processing Purposes

Legitimate Business Purposes

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

(a) Hosting, storage, and other Processing needed for business continuity and disaster recovery, including making back-up and Archive copies of Personal Data;

(b) System and network administration and security, including infrastructure monitoring, identity and credential management, verification and authentication, and access control;

(c) Monitoring and other controls needed to safeguard the security and integrity of transactions (e.g. financial transactions and money movement activities) including for due diligence (such as verifying the identity of the Individual, and the Individual's eligibility to receive products or services (such as verifying employment or account status);

(d) Enforcing contracts and protecting ADP, its Associates, Clients, Client Employees, and the public against theft, legal liability, fraud, or abuse including: (i) detecting, investigating, preventing, and mitigating the harm from actual and attempted financial fraud, identity fraud, and other threats against financial and physical assets, access credentials, and information systems; (ii) participating in external cybersecurity, anti-fraud and anti-money laundering initiatives; and (iii) as needed to protect the vital interests of Individuals, such as by alerting Individuals to an observed security threat;

(e) ADP internal business process execution and management leading to incidental Processing of Client Data for:

(1) Internal auditing and consolidated reporting;

(2) Legal compliance, including mandatory filings, uses, and disclosures of information that are required by Applicable Law;

(3) Data de-identification and aggregation of de-identified data for data minimization and services analyses;

(4) Use of de-identified and aggregated data, as permitted by Clients, to facilitate analytics, continuity and improvement of ADP products and services; and

(5) Facilitating corporate governance, including mergers, acquisitions, divestitures, and joint ventures.

Article 5 – Security Requirements

Data Security **5.1** ADP shall employ commercially reasonable and appropriate technical, physical, and organizational measures to protect Client Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access during the Processing, which will meet the requirements of EEA Applicable Law, or any stricter requirements, as imposed under the Service Agreement. ADP shall, in any event, take the measures specified in Annex 2 of this Code, which measures may be modified by ADP, provided that such changes do not materially diminish the level of security provided to Client Data under Annex 2.

Data Access and Confidentiality **5.2** Staff shall be authorized to access Client Data only to the extent necessary to serve the applicable data processing purposes under Article 4. ADP shall impose confidentiality obligations on Staff who have access to Client Data.

Data Security Breach Notification **5.3** ADP shall notify the Client of a Data Security Breach without undue delay after becoming aware that such a breach has occurred, unless a law enforcement official or supervisory authority determines that notification would impede a criminal investigation, or cause damage to national security or a breach of trust in the relevant industry sector. In this case, notification shall be delayed as instructed by such law enforcement official or supervisory authority. ADP shall respond promptly to Client inquiries relating to said Data Security Breach.

Article 6 – Transparency to Client Employees

Other Requests of Client Employees **6.1** ADP shall promptly notify the Client of requests or complaints related to the Processing of Personal Data by ADP that are received directly from Client Employees without responding to such requests or complaints, unless otherwise provided in the Service Agreement or instructed by the Client.

If instructed by the Client to respond to Client Employee requests and complaints in the Service Agreement, ADP shall ensure that Client Employees are provided with all information reasonably required (such as the point of contact and the procedure) in order for the Client Employee to be able to effectively make the request or lodge the complaint.

The provisions of this Article 6.1 shall not apply to requests that are handled by ADP in the normal course of providing Client Services and Client Support Activities.

Article 7 – Subprocessors

Third Party Subprocessing Contracts **7.1** Third Party Subprocessors may only Process Client Data pursuant to a Subprocessor Contract. The Subprocessor Contract shall impose similar data protection-related Processing terms on the Third Party Subprocessor that will be not less protective than those imposed on the ADP Contracting Entity by the Service Agreement and this Code.

Publication of Overview of Subprocessors **7.2** ADP shall publish an overview of the categories of Subprocessors involved in the performance of the relevant Client Services on the appropriate ADP website. This overview shall be promptly updated in case of changes.

Notification of New Subprocessors and Right to Object **7.3** ADP shall provide notice to the Client of any new Subprocessors engaged by ADP for the delivery of the Client Services. Within 30 days of receiving such notice, the Client may object to such Subprocessor by providing written notice to ADP alleging objective justifiable grounds related to the inability of such Subprocessor to protect Client Data in accordance with the related obligations of the Subprocessor Contract, as referred to in Article 7.1. In the event that the parties cannot reach a mutually acceptable solution, ADP shall, at its option, refrain from allowing the Subprocessor to access the Client Data, or enable the Client to terminate the relevant Client Services in accordance with the terms of the Service Agreement.

Exception **7.4** The provisions of this Section 7 shall not apply to the extent the Client instructs ADP to allow a Third Party to Process Client Data pursuant to a contract that the Client has directly with the Third Party (e.g., a Third Party benefits provider).

Article 8 – Supervision and Compliance

Global Chief Privacy Officer **8.1** 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 Client 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) Monitoring the process by which Privacy Impact Assessments (PIAs) are conducted and reviewing PIAs as appropriate;

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

(i) 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 Client Data;

(3) Providing, assisting, or advising on the privacy training to Staff so 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; and

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

Privacy Network **8.2** 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 8.1 and other tasks as may be appropriate to maintain and update this Code. The members of the Privacy Network, as relevant to their role in the region or organization, shall perform 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 their 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 Client 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 assist with the resolution of these complaints; 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 products and services are implemented in the Group Companies or organizations; and

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

Privacy Stewards **8.3** Privacy Stewards are ADP executives who have been appointed by a Responsible Executive and/or ADP's Executive Leadership to implement and enforce the Code 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 Client Data, and that adequate resources and budget are available to meet the obligations of this Code. Privacy Stewards may delegate tasks and shall allocate appropriate resources as needed to meet their responsibilities and achieve compliance goals.

The 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;

(e) Monitoring Subprocessors used by the Group Company, business unit, or functional area to confirm ongoing compliance by the Subprocessors with this Code and the Subprocessors' Contracts;

(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 Client Data be deleted, destroyed, de-identified, or transferred as required by Article 2.2.

Responsible Executives

8.4 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

8.5 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 Group Companies, business units, and 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

8.6 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 set forth in Article 8.2.

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 8.3.

Statutory Positions **8.7** 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 9 – Policies and Procedures

Policies and Procedures **9.1** ADP shall develop and implement policies, standards, guidelines, and procedures to comply with this Code.

System Information **9.2** ADP shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Client Data, such as inventories of systems and processes that impact Client 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 for Client under Article 11.3 upon request.

Article 10 – Training

Training **10.1** ADP shall provide training on the obligations and principles set forth in this Code, and other privacy and data security obligations to all Staff with access to Client Data or responsibilities associated with Processing Client Data.

Article 11 – Monitoring and Auditing Compliance

Internal Audits **11.1** ADP shall audit business processes and procedures that involve the Processing of Client Data for compliance with this Code on a regular basis. 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), and 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 Lead DPA or to a DPA competent under Article 11.3 upon request.

Client Audit

11.2 ADP will address Client audit requests as described in this Article 11.2. ADP will answer questions asked by the Client regarding the Processing of Client Data by ADP. In the event the Client reasonably considers that the answers provided by ADP justify further analysis, ADP shall, in agreement with the Client, either:

(a) Make the facilities it uses for the Processing of Client Data available for an audit by a qualified independent third party assessor reasonably acceptable to ADP and bound by confidentiality obligations satisfactory to ADP, and engaged by the Client. The Client will provide a copy of the audit report to the Global Chief Privacy Officer which shall be treated as ADP confidential information. Audits shall be conducted no more than once per year, per Client, during the term of the Service Agreement, during regular business hours, and shall be subject to (i) a written request submitted to ADP at least 45 days in advance of the proposed audit date; (ii) a detailed written audit plan reviewed and approved by ADP's security organization; and (iii) ADP's on-site security policies. Such audits will take place only in the presence of a representative of ADP's Global Security Office, ADP's Global Data Privacy and Governance Team, or such person designated by the appropriate representative. The audits shall not be permitted to disrupt ADP's Processing activities or compromise the security and confidentiality of Personal Data pertaining to other ADP Clients; or

(b) ADP shall provide a statement to the Client issued by a qualified independent third party assessor certifying that the ADP business processes and procedures that involve the Processing of Client Data comply with this Code.

ADP may charge Clients a reasonable fee for such audit.

This Article 11.2 supplements or clarifies the audit rights which Clients may have under Applicable Law and Service Agreements. In case of contradiction, the provisions of Applicable Law and Service Agreements shall prevail.

Audits by DPAs **11.3** Any DPA of an EEA Country which is competent to audit an ADP Client will be authorized to audit the relevant data transfer for compliance with this Code, under the same conditions as would apply to an audit by that DPA of the Client itself under the Applicable Data Controller Law.

To facilitate any such audit:

(a) ADP and the Client will collaborate in good faith to attempt to resolve the request by providing information to the DPA, such as ADP audit reports, and shall facilitate discussions between the DPA, and the Client's and ADP's subject matter experts, who can review the security, privacy, and operational controls that are in place. The Client will have access to its Client Data in accordance with the Service Agreement, and may delegate such access to representatives of the DPA;

(b) 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;

(c) If this appears insufficient, ADP will provide the DPA with a direct right to examine ADP's data processing facilities used to Process Client Data on reasonable prior notice, during business hours, and with full respect to the confidentiality of the information obtained and to the trade secrets of ADP. The DPA can only access the Client Data belonging to the Client.

This Article 11.3 supplements or clarifies the audit rights which DPAs may have under Applicable Law and Service Agreements. In case of contradiction, the provisions of Applicable Law shall prevail.

Annual Report **11.4** The Global Chief Privacy Officer shall produce an annual report for the ADP Executive Committee on compliance with this Code, privacy, 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 **11.5** ADP shall take appropriate steps to address any instances of non-compliance with this Code identified during compliance audits.

Article 12 – Legal Issues

Rights of Client Employees

12.1 If ADP violates the Code with respect to the Personal Data of a Client Employee covered by this Code, such Client Employee can as a third party beneficiary enforce Articles 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8, and 14.3 of this Processor Code against the ADP Contracting Entity.

To the extent the Client Employee may enforce any such rights against the ADP Contracting Entity, the ADP Contracting Entity may not rely on a breach of its obligations by a Subprocessor to avoid liability, except to the extent that a defense of a Subprocessor would also constitute a defense of ADP. ADP may, however, assert any defenses or rights that would have been available to the Client. ADP also may assert any defenses that ADP could have asserted against the Client (such as contributory negligence), in defending against the affected Individual's claim.

Complaint Procedure

12.2 Client Employees may file a written complaint in respect of any claim they have under Article 12.1 with the Global Data Privacy and Governance Team via mail or email at the address indicated at the end of this Code. Client Employee may also file a complaint or claim with the authorities or the courts in accordance with Article 12.3 of this Code.

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.

ADP will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Client Employee within four weeks of the date that the complaint was filed. The response will be in writing and will be sent to the Client Employee via the means that the Client Employee 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 Client Employee within four weeks that the investigation is ongoing and that a response will be provided within the next eight week period.

If ADP's response to the complaint is unsatisfactory to the Client Employee (e.g., the request is denied) or ADP does not observe the conditions of the complaints procedure set out in this Article 12.2, the Client Employee can file a complaint or claim with the authorities or the courts in accordance with Article 12.3.

Jurisdiction for Claims of Client Employees

12.3 Client Employees are encouraged to first follow the complaints procedure set forth in Article 12.2 of this Code before filing any complaint or claim with the authorities or the courts.

Client Employees may, at their choice, submit claims under Article 12.1 by bringing a complaint to
(i) the DPA in the country of his/her habitual residence, place of work or place where the infringement took place, against the ADP Contracting Entity or the ADP Delegated Entity; or
(ii) the Lead DPA or the courts in the Netherlands, but in that case, only against the ADP Delegated Entity.

Client Employees may, at their choice, submit claims under Article 12.1 by bringing a complaint to:
(i) the courts in the country of his/her habitual residence, or the country of origin of the data transfer under this Code, against the ADP Contracting Entity or the ADP Delegated Entity; or
(ii) the Lead DPA or the courts in the Netherlands, but in that case, only against the ADP Delegated Entity.

The DPAs and courts shall apply their own substantive and procedural laws to the disputes. The choice made by the Client Employee will not prejudice the substantive or procedural rights that the parties may have under Applicable Law.

Rights of Clients

12.4 The Client may enforce this Code against (i) the ADP Contracting Entity or, (ii) the ADP Delegated Entity before the Lead DPA or the courts in the Netherlands, but only if the ADP Contracting Entity is not established in an EEA Country. The ADP Delegated Entity shall ensure that adequate steps are taken to address violations of this Code by the ADP Contracting Entity, or any other Group Company involved.

The ADP Contracting Entity and the ADP Delegated Entity may not rely on a breach of its obligations by another Group Company or a Subprocessor to avoid

liability, except to the extent that a defense of such Group Company or Subprocessor would also constitute a defense of ADP.

Available Remedies, Burden of Proof for Client Employees **12.5** In the event that a Client Employee has a claim under Article 12.1, Client Employee shall be entitled to compensation of any damages to the extent provided by applicable EEA law.

If Client Employees bring claims for damages under Article 12.1, the onus will be on the Client Employees to demonstrate that they have suffered damage, and to establish facts which show it is plausible that the damage has occurred because of a violation of this Code. Subsequently, the ADP Contracting Entity (or the ADP Delegated Entity, as applicable) will have the burden to prove that the damages suffered by the Client Employees due to a violation of this Code are not attributable to the relevant Group Company or a Subprocessor, or to assert other applicable defenses.

Client Compensation **12.6** In case of a violation of this Code, and subject to the terms of the Service Agreement, Clients shall be entitled to compensation of direct damages consistent with the provisions of the Service Agreement.

Mutual assistance **12.7** All Group Companies shall, as needed, co-operate and assist to the extent reasonably possible with (a) handling a request, complaint, or claim made by a Client or a Client Employee or (b) complying with a lawful investigation or inquiry by a competent government authority.

The Group Company receiving a request for information pursuant to Article 6.1, or a complaint or claim pursuant to Article 12.2 or 12.3, is responsible for handling any communication with the Client or with the Client Employee regarding the request or claim, except where circumstances dictate otherwise, or as directed by the Global Data Privacy and Governance Team.

DPA Advice and Binding Decisions **12.8** 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 12.3 issued on the interpretation and application of this Code. ADP shall abide by binding decisions of competent DPAs.

Law Applicable to this Code **12.9** This Code shall be governed by and interpreted in accordance with Dutch law.

Article 13 – Sanctions for Non-compliance

Non-compliance **13.1** Non-compliance of Staff with this Code may result in appropriate disciplinary or contractual measures in accordance with applicable law and ADP policies, up to and including termination of the employment relationship or contract.

Article 14 – Conflicts between this Code and Applicable Data Processor Law

Conflict between this Code and Law **14.1** Where there is a conflict between Applicable Data Processor 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 to resolve the conflict to the extent reasonably practicable given the legal requirements applicable to ADP.

New Conflicting Legal Requirements **14.2** 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 of which they become aware 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 Executives of any new legal requirement that may interfere with ADP's ability to comply with this Code.

Reporting to Lead DPA **14.3** If ADP becomes aware that Applicable Data Processor Law or any change in Applicable Data Processor Law is likely to have a substantial adverse effect on ADP's ability to meet its obligations under 3.1, 3.2 or 11.3, ADP will report this to the Lead DPA.

Article 15 – Changes to this Code

Approval for Changes

15.1 Any material changes to this Code require the prior approval of the Global Chief Privacy Officer and the General Counsel, and adoption by the ADP Executive Committee and shall thereafter be communicated to Group Companies. Non-material changes to the Code may be made upon the prior approval of the Global Chief Privacy Officer. The ADP Delegated Entity shall notify the Lead DPA of changes to this Code on an annual basis.

Where a change to this Code has a significant impact on the Processing conditions of the Client Services, ADP will promptly inform the Lead DPA thereof including a brief explanation for such change as well as provide notice of such change to the Client. Within 30 days of receiving such notice, the Client may object to such change by providing written notice to ADP. In the event that the parties cannot reach a mutually acceptable solution, ADP shall put in place an alternative data transfer solution. In the event no alternative data transfer solution can be put in place, the Client will have the right under this Code to suspend the relevant transfer to ADP of Client Data. In the event a suspension of the data transfers is not possible, ADP shall enable the Client to terminate the relevant Client Services in accordance with the terms of the Service Agreement.

Effective Date Of Changes

15.2 Any change shall enter into force with immediate effect after it has been approved in accordance with Article 15.1, published on the www.adp.com website, and communicated to the Clients.

Prior Versions

15.3 Any request, complaint, or claim of a Client Employee involving this Code shall be judged against the version of this Code that is in force at the time the request, complaint, or claim is made.

Article 16 – Implementation and Transition Periods

Implementation

16.1 The implementation of this Code shall be supervised by the 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 1.6) for compliance with this Code.

Accordingly, except as otherwise indicated, within eighteen months of the Effective Date, all Processing of Client 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.

New Group Companies **16.2** 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 **16.3** A Divested Entity will remain covered by this Code after its divestment for such period as is required by ADP to disentangle the Processing of Client Data related to such Divested Entity.

Transition Period for Existing Agreements **16.4** Where there are existing agreements with Subprocessors or other 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 18 months 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, such as the Privacy Shield, 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, LLC.
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 Individual. 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 is 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 is 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. 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, LLC., if either Automatic Data Processing, Inc. or ADP, LLC. 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.
Services Agreement	SERVICES 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 – Security Measures

Presented by:	**ADP - Global Security Organization**
Version:	**1.8**
Released:	**October 2018**

Contents

1. Information Security Policies 34
   - A. Information Security Management 34
   - B. Independence of Information Security Function 34
   - C. Formal Definition of an Information Security Policy 34
   - D. Information Security Policy Review 35
2. Organization of Information Security 36
   - A. Information Security Roles and Responsibilities 36
   - B. Mobile Computing and Teleworking Policy 36
3. Human Resource Security 37
   - A. Background Checks 37
   - B. Confidentiality Agreements with Employees and Contractors 37
   - C. Information Security Training Program 37
   - D. Security Awareness of Employee and Contractors 37
   - E. Employees Responsibilities and Disciplinary Processes 37
   - F. Termination of Employment Responsibilities 38
4. Asset Management 39
   - A. Acceptable Use of Assets 39
   - B. Classification of Information 39
   - C. Equipment and Media Disposal 39
   - D. Physical Media in Transit 40
5. Access Control 41
   - A. Business Requirements of Access Control 41
   - B. Access to Infrastructure - Access Control Management 41
   - C. Password policy 42
   - D. Session Timeouts 42
6. Cryptography 43
   - A. Cryptographic Controls 43
   - B. Key Management 43
7. Physical and Environmental Security 44
   - A. Physical Security 44
   - B. Physical Access Control Mechanisms 44
   - C. Review of Access to Sensitive Areas 44
   - D. Identification of ADP Personnel 45
   - E. Physical and Environmental Security Controls in Data Centers 45
8. Operations Security 46
   - A. Formalization of IT Operations Procedures 46
   - B. Infrastructure Change Management 46
   - C. System Capacity Planning and Acceptance 46
   - D. Protection against Malicious Code 46

E. Back-Up Management Policy 46
F. Security Logging and Monitoring 47
G. Infrastructure Systems and Monitoring 47
H. Technical Vulnerability Management 48
9. Communications Security 49
A. Network Security Management 49
B. Exchange of Information 49
C. Use of Messaging Systems 49
10. System acquisition, development, and maintenance 50
A. Security in Development and Support Processes 50
B. Security in Development Environment 50
C. Test Data 51
11. Supplier relationships 52
A. Identification of Risks Related to External Parties 52
B. Information Security Agreements with External Parties 52
12. Information Security Incident Management 53
A. Management of Information Security Incidents and Improvements 53
13. Information Security Aspects of Business Resiliency Management 54
A. ADP Business Resiliency Program 54
B. Implementation of Business Resiliency 55
C. Availability of Disaster Recovery Facilities 56
14. Compliance 57
A. Compliance with Legal Requirements 57
B. Compliance with Security Policies and Standards 57
C. Technical Compliance 57
D. Retention of Data 58
15. Appendix 59
A. Logical Network Diagram 59

Terms and Definitions

The following terms may appear throughout the document:

Term or Acronym used	Definition
PTSS	**GSO's Preventative Technical Security Services**
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
LDAP	**Lightweight Directory Access Protocol**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Document History

Version	Release date	Author/Sponsor	Revision Summary
1.0	Aug 2013	ADP Global Security Organization	Original Version
1.1	Jan 2014	ADP Global Security Organization	Minor updates
1.2	Dec 2014	ADP Global Security Organization	Update to LLC
1.3	Feb 2015	Client Security Management Office	Revised to ISO 27001:2013 to fit for EMEA
1.4	Jan 2016	ADP Global Security Organization / ADP Legal Department	Revised to fit GES EMEA and MNC in the same document
1.5	Jun 2017	Client Security Management Office	Minor updates
1.6	Sep 2017	Client Security Management Office	Document globalization
1.61	Sep 2017	Client Security Management Office	Minor update
1.7	Feb 2018	Client Security Management Office	Minor update
1.8	Oct 2018	Client Security Management Office	Minor updates

Overview

ADP maintains a formal information security program containing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of client information. This program is reasonably designed to (i) safeguard the security and confidentiality of client information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information.

This document contains an overview of ADP's information security measures and practices, as of the release date and which are subject to change by ADP. These requirements and practices are designed to be consistent with the ISO/IEC 27001:2013 information security standards. References to the corresponding sections of ISO 27001 are included in each section in [italics].

ADP periodically assesses its security policies, standards. Our goal is to ensure that the security program effectively and efficiently operates to protect all of the information entrusted to us by our clients and their employees.

1. Information Security Policies

A. Information Security Management

ADP is committed to ensuring that information security is properly managed and that the measures described in this document are implemented and appropriately adhered to by ADP staff and applicable third parties.

B. Independence of Information Security Function

ADP has a Chief Security Officer who oversees ADP's Global Security Organization (GSO) and reports to Chief Financial Officer, instead of to the Chief Information Officer, which gives GSO the necessary independence from IT. The GSO is a cross-divisional security team that creates a multi-disciplinary approach in the areas of cyber and information security and compliance, operational risk management, client security management, workforce protection, and business resilience. GSO senior management, under our Chief Security Officer are responsible for managing security policies, procedures and guidelines.

C. Formal Definition of an Information Security Policy

[5.1.1] Policies for information security

ADP has developed and documented formal information security policies that set out ADP's approach to managing information security.

Specific areas covered by this policy include, but are not limited to the following:

- **Security, Risk and Privacy Management Policy –** Reviews the responsibilities of the Global Security Organization ("GSO"), the Chief Security Officer ("CSO") and the Global Chief Privacy Officer ("GCPO").
- **Global Privacy Policy -** Discusses the collection of personal information, access to, accuracy, disclosures, and privacy statement to clients.
- **Information Security Responsibilities for Associates and Managers Policy –** Includes the Information Security Responsibilities and controls on hiring process from a security perspective.
- **Acceptable Use of Electronic Communications and Data Protection Policy** – Discusses acceptable use, different electronic communications, encryption, and key management.
- **Information Handling and Classification Policy –** Provides requirements for the classification of ADP information and establishes protection controls.
- **Physical Security Policy–** Examines the security of ADP facilities and subsequently our Associates and visitors who work there.
- **Security Operations Management Policy –** Provides minimum controls for maintaining system patches, effectively address the threat from malware, and maintain backups and database security controls.
- **Security Monitoring Policy –** Provides controls for intrusion detection systems (IDS), logs, and data loss prevention (DLP).
- **Investigations, Electronic Discovery and Incident Management Policy –** This covers: incident response, EDILS, workforce protection, access to associates electronic stored information.
- **Access & Authentication Policy –** Covers authentication (e.g. user ID and password), remote access and wireless access.
- **Network Security Policy –** Security architecture of routers, firewalls, AD, DNS, email servers, DMZ, cloud services, network devices, web proxy, and switched network technology.
- **Global Vendor Assurance Policy –** Sets minimum security controls for engaging any third party to assist ADP in achieving its business objectives.

- **Application Management Policy –** Establishes appropriate security controls into each stage of the system development lifecycle.
- **Business Resiliency Policy –**Ensures the protection, integrity and preservation of ADP by establishing the minimum requirements to document, implement, maintain and continually improve Business Resiliency Programs
- **Operational Risk Management Policy –** Identification, monitoring, response, analysis, governance, and new business initiatives.

Policies are published in the Associate Portal and are accessible to all employees and contractors from within ADP network.

D. Information Security Policy Review

[5.1.2] Review of the policies for information security

ADP reviews its information security policy at least once a year or whenever there are major changes impacting the functioning of ADP's information systems.

2. Organization of Information Security

A. Information Security Roles and Responsibilities

[6.1.1] Information security roles and responsibilities

The GSO consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined in writing for all members of the GSO. The GSO is charged with the design, implementation and oversight of our information security program based on corporate policies. The GSO's activities are overseen by the Executive Security Committee, composed of the Chief Security Officer, the Chief Executive Officer, the Chief Financial Officer, the Chief Information Officer, Chief Human Resources Officer and the General Counsel.

B. Mobile Computing and Teleworking Policy

[6.2.1] Mobile device policy

[6.2.2] Teleworking

ADP requires all confidential information to be encrypted on mobile devices, in order to prevent any data leakage resulting from a theft or a loss of a computer. Antivirus software, with updated virus signature files and two-factor authentication over VPN is also required to access the corporate networks remotely. All remote devices are required to be password protected.

ADP employees are required to report lost or stolen remote computing devices immediately through a Security Incident Reporting Process.

All employees and contractors, as a condition of employment with ADP, must comply with the ADP's acceptable use and other relevant Policies.

3. Human Resource Security

A. Background Checks

[7.1.1] Screening

Consistent with applicable legal requirements in the individual's jurisdiction, ADP conducts appropriate background checks commensurate with the duties and responsibilities of its employees, contractors and/or third parties to ensure their suitability for handling clients' information prior to engaging or hiring such individuals.

Background screening may include the following components:

a) Identity/employment eligibility verification
b) Employment history
c) Educational history and professional qualifications
d) Criminal records (where legally authorized and depending on local country regulations)

B. Confidentiality Agreements with Employees and Contractors

[7.1.2] Terms and conditions of employment

ADP employment contracts and contracts with contractors contain terms setting out an appropriate catalogue of obligations and responsibilities concerning client information to which they will have access. All ADP employees and contractors are bound by confidentiality obligations.

C. Information Security Training Program

[7.2.2] Information security awareness, education and training

ADP ensures that all personnel scheduled to access and/or otherwise process ADP's clients' information, are provided with information security and privacy awareness training with the objective to promote effective privacy and security practices.

All employees receive information security training as part of their on boarding plan. In addition, ADP delivers annual security training in order to remind employees of their responsibilities when performing their day-to-day duties.

D. Security Awareness of Employee and Contractors

[7.2.2] Information security awareness, education and training

The ADP information security policy document is approved by management, published and communicated to all employees, onsite contractors and applicable third parties.

ADP employees and onsite contractors are required to comply with the Information Security Responsibilities and associated information security policies.

E. Employees Responsibilities and Disciplinary Processes

[7.2.3] Disciplinary process

ADP has published a security policy that all ADP associates need to comply with. Violations of security policies may lead to revocation of access privileges and/or disciplinary actions up to and including termination of consulting contracts or employment.

F. Termination of Employment Responsibilities

[7.3.1] Termination or change of employment responsibilities

[8.1.4] Return of assets

[9.2.6] Removal or adjustment of access rights

Responsibilities upon termination of employment have been formally documented and include at least:

a) Return all ADP information and assets in the possession of the respective employee, on whatever medium it is stored
b) Termination of access rights to ADP facilities, information and systems
c) Change of passwords for remaining active shared accounts, if applicable
d) Transfer of knowledge, if applicable.

Access rights of all ADP employees and contractors to data and data processing facilities are removed upon termination of their contract with ADP.

4. Asset Management

A. Acceptable Use of Assets

[8.1.3] Acceptable use of assets

Acceptable use of assets is articulated across several policies, applicable to ADP employees and contractors, in order to ensure that ADP's and clients' information are not exposed by use of such assets. Examples of areas described in these policies are: use of electronic communications, use of electronic equipment, and use of information assets.

B. Classification of Information

[8.2.1] Classification of information

Information acquired, created or maintained by or on behalf of ADP is assigned, as applicable, a security classification of:

- Public
- ADP Internal Use Only
- ADP Confidential
- ADP Restricted

Requirements for handling information are directly correlated to the information security classification.

Personal Information and Sensitive Personal Information are considered in all cases ADP Confidential.

ADP employees are accountable for protecting and handling information assets in accordance with their security classification level, which provides protection of information and applicable handling requirements for each classification level. All client information is classified as confidential.

The ADP confidentiality classification is applied to all information stored, transmitted or handled by third parties.

C. Equipment and Media Disposal

[8.3.1] Management of removable media

[8.3.2] Disposal of media

When ADP equipment, documents, files, and media are disposed of or reused, appropriate measures are taken to prevent subsequent retrieval of client's information originally stored in them.

All information on computers or electronic storage media regardless of classification is overwritten or degaussed, unless the media is physically destroyed before being released outside ADP facilities.

The procedures for ensuring the secure destruction/erasure of ADP information held on equipment, in documents, files, and media are formally documented.

D. Physical Media in Transit

[8.3.3] Physical media transfer

Organizational measures are taken to ensure that printed materials containing clients' information cannot be viewed by unauthorized individuals.

Measures are also taken to protect printed materials containing clients' information against theft, loss, and/or unauthorized access/modification (i) during transit e.g. sealed envelopes, containers and hand delivery to authorized user; and (ii) during review, revision or other processing where removed from secure storage.

5. Access Control

A. Business Requirements of Access Control

[9.1.1] Access control policy

ADP's Access control policy is based on business defined requirements. The policies and control standards are articulated into access controls enforced in all components of the provided service and are based on a "least-privilege" and "need to know" principle.

B. Access to Infrastructure - Access Control Management

[9.2.1] User registration and de-registration

[9.2.2] User access provisioning

[9.2.5] Review of user access rights

[9.4.3] Password management system

Access requests to move, add, create and delete are logged, approved and periodically reviewed.

A formal review is performed at least yearly to make sure individual users correspond correctly to the relevant business role and would not have continued access after a position change. This process is audited and documented in a SOC1[1] type II report.

From within an Identity Management System, a dedicated ADP team is responsible for granting, denying, cancelling, terminating and decommissioning/deactivating any access to ADP facilities and information systems.

Administrator access is only possible from ADP internal network or equivalent through a secure remote VPN access using two-factor authentication.

For the UNIX domain, access to privilege accounts is based on a "need to know" principle. All access requests are validated by the Security Team and an audit trail is maintained.

For the Windows domain, user accounts are defined in a central Active Directory (AD). The AD for servers in production is different from the AD used for workstations.

ADP uses a centralized identity and access management (IAM) tool that is managed centrally by a dedicated GETS team. According to the access rights requested through the centralized IAM tool, a validation workflow will be triggered that could involve the users' supervisor. Access is provided on a temporary basis and workflows exist to prevent such access from remaining permanent.

An employee's access to a facility is decommissioned immediately after the last day of employment by deactivating their access card (employee badge). The employee's user IDs are immediately deactivated.

Any employee's assets will be returned and checked by the competent line manager against the asset list present in the configuration management data base.

Following a job position change, or organizational changes, user profiles or user access rights are required to be modified by the applicable business unit management and the IAM Team. Additionally, a formal review of access rights is performed every year to verify that individual users' rights correspond to their relevant business role and that there are no remaining irrelevant access rights after a position transfer.

[1] In the case of certain US Services offered by ADP, this is audited in a SOC 2 Type 2 report.

C. Password policy

[9.1.1] Access control policy

[9.4.2] Secure log-on procedures

[9.4.3] Password management system

ADP associate password policies are enforced in servers, databases and network devices and applications, to the extent the device/application allows it. The password complexity is derived from a risk based analysis of the protected data and content.

The policies meet prevailing industry standards for strength and complexity, and include a minimum password length of 8 characters, with password composition of 1 or more characters from at least 3 of the following 4 classes:

- English upper case letters (e.g., A, B, C, ...Z)
- English lower case letters (e.g., a, b, c, ...z)
- Digits (e.g., 0, 1, 2, ...9)
- Non-alphanumeric special characters (e.g., ?,!,%,$,#, etc.)

Additionally, ADP associate passwords must be compliant with the following rules:

- Passwords are changed at regular intervals according to the sensitivity of the information accessible through the systems to which they relate in accordance with ADP global security policies
- Passwords are stored using one-way hash with “salt”
- Passwords must not contain the user ID in the password
- Passwords must not contain the user's first and/or last name
- Maximum of 4 repeating characters in the password
- Previous 4 passwords cannot be reused
- There is a list of prohibited passwords
- Passwords can be changed only once per day
- Password expire after 90 days
- User is disabled after 180 days of inactivity
- Account is locked after 4 failed logon attempts

Client application authentication requirements vary by product, and federated services (SAML 2.0) is available on specific ADP applications using a unified network and security layer managed by GETS.

D. Session Timeouts

[A.9.4.1] Information access restriction

ADP enforces automatic timeouts to all servers, workstations, applications and VPN connections.

- Server session: timeout after 20 minutes of inactivity.
- Workstation session (laptops, PCs, terminals, etc.): timeout after 20 minutes of inactivity.
- Applications: all applications have a timeout after a period of inactivity, which will vary depending on the application.
- VPN session: timeout after no longer than 24 hours of usage.

Re-establishment of sessions may take place only after the user has provided a valid password.

6. Cryptography

A. Cryptographic Controls

[10.1.1] Policy on the use of cryptographic controls

ADP requires that sensitive information being exchanged between ADP and ADP third parties must be encrypted (or transport channel must be encrypted) using industry accepted encryption techniques and strengths. Alternatively, a private leased line must be used.

B. Key Management

[10.1.2] Key management

ADP has an internal Encryption Security Standard that includes well-defined key management and key escrow procedures, including both symmetric and asymmetric keys management.

Encryption keys used for ADP information are always classified as confidential information. Access to such keys is strictly limited to those who have a need to know and, unless an exception approval is provided, encryption keys are not revealed to consultants, contractors, temporary associates, or third parties.

For encryption, copies of server certificates are exported and secured. Certificates are managed via a VeriSign Global Server account.

7. Physical and Environmental Security

A. Physical Security

[11.1.1] Physical security perimeter

[11.1.3] Securing offices, rooms and facilities

ADP ensures that designated workspaces for payroll processing and information processing facilities are physically isolated from the rest of the facility through the use of secured access controls and walls extending from floor to ceiling.

B. Physical Access Control Mechanisms

[11.1.2] Physical entry controls

ADP facilities

Access to ADP facilities requires electronic security badges using card key authentication and the maintenance of physical access logs to the premises.

Any access, including access to sensitive areas of ADP facilities, such as server rooms and tape libraries, is controlled by Electronic Access Control (EAC) mechanisms.

Data Centers

ADP hosting infrastructures are all contained within physically secured environments. Access to the hosting center requires electronic security badges using card key and pin or biometric authentication and the maintenance of a physical access logs to the premises.

C. Review of Access to Sensitive Areas

[9.2.1] User registration and de-registration

[11.1.2] Physical entry controls

ADP facilities

Access to ADP facilities and sensitive areas is restricted to ADP employees and other authorized persons. Access to facility resources is granted on the basis of each individual's work responsibilities.

Audit trails are kept of all admissions in and out of all buildings and sensitive areas. Audit trails are maintained and reviewed as appropriate.

Data Centers

The data center security officer and/or facilities manager is/are responsible for managing access rights to any ADP data center. ADP is responsible for maintaining and controlling access to ADP areas according to a pre-approved list.

Audit trails are kept of all admissions in and out of data centers. Audit trails are maintained and reviewed by hosting center management and audit personnel on a monthly basis.

In order to gain admittance into the data centers, all visitors must be announced in advance and accompanied by authorized personnel once in the facility.

ADP management reviews the accuracy and appropriateness of physical access rights to ADP data centers monthly and for other ADP facilities at least on an annual basis. Access is removed when an employee leaves ADP.

D. Identification of ADP Personnel

[11.1.5] Working in secure areas

ADP facilities

All ADP personnel must wear and display their identification badges at all times within ADP facilities. Visitors are required to sign a visitors' log, wear a visitor badge and be escorted by ADP personnel.

Data Centers

All ADP personnel, clients, contractors, and visitors must wear and display data center's identification badge at all times within the data center. Clients, contractors, and visitors are required to be accompanied by authorized personnel.

Tailgating or any similar practices of allowing an unauthorized person to enter behind or along with an authorized cardholder, or attempting to enter where a cardholder has not been granted access, are prohibited.

E. Physical and Environmental Security Controls in Data Centers

[11.1.4] Protecting against external and environmental threats

ADP data center facilities are monitored using controls of environmental conditions, surveillance cameras, motion detection cameras and security guards. All facilities utilize entry alarms.

Physical and environmental controls against reasonably anticipated site specific disasters such as flood and fire have been applied to ADP data centers.

ADP data centers have a minimum of the following environmental and physical security controls:

a) Redundant HVAC (heating, ventilation, and air conditioning) systems
b) Temperature/humidity monitoring
c) Local and remote alarms (power, temperature, humidity)
d) N+1 UPS
e) Redundant power supply
f) Automatic fire detection alarm
g) Automatic fire suppression
h) Additional manual fire suppression mechanisms
i) Servers located in protected areas

Cables and wires connected to or coming from computing equipment and peripherals are routed to minimize damage. Power distribution cabling for the computer equipment is located in trays under a raised floor or in conduits routed above the suspended ceiling. Only dedicated staff from hosting center and authorized support personnel can access phone/cable closets. Equipment is continuously monitored by automatic systems. All incidents are reviewed on a daily basis and corrective actions, such as replacement of equipment, are taken, as necessary. Appropriate change management controls also apply to equipment replacement.

8. Operations Security

A. Formalization of IT Operations Procedures

[12.1.1] Documented operating procedures

GETS is the ADP unit responsible for IT infrastructure operations and maintenance. GETS formally maintains and documents IT operations policies and procedures. These procedures include, but are not limited to the following:

a) Change management
b) Back-up management
c) System error handling
d) System restart and recovery
e) System monitoring
f) Jobs scheduling and monitoring

B. Infrastructure Change Management

[12.1.2] Change management

A periodic Change Advisory Board (CAB), including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place to discuss impacts, to agree on deployment windows and to approve the promotions to production, as well as to coordinate any other change in the production infrastructure.

C. System Capacity Planning and Acceptance

[12.1.3] Capacity management

Capacity requirements are continuously monitored and regularly reviewed. Following these reviews, systems and networks are scaled up or down accordingly.

When significant changes have to be performed due to a change in capacity or a technological evolution, the GETS benchmarking team can perform stress tests to the relevant application and/or system, thus providing a detailed report of performance evolution by gauging the changes in (i) components, (ii) system configuration or version, or (iii) middleware configuration or version.

D. Protection against Malicious Code

[12.2.1] Controls against malware

Antivirus software is installed on all computer systems connected to an ADP network, and virus signatures are updated automatically and periodically as per vendor updates and release schedule.

E. Back-Up Management Policy

[12.3.1] Information backup

ADP has policies in place that require all production hosting operations to back-up production information. The scope and the frequency of back-ups are executed in accordance with the business requirements of relevant ADP services, the security requirements of the information involved, and the criticality of the information in respect of disaster recovery.

According to those requirements, the following back-ups are performed:

a) Daily incremental back-ups
b) Weekly full back-ups
c) Monthly full back-ups

Monitoring of scheduled back-ups is performed by GETS, in order to identify back-up issues or exceptions. Any issue identified or abnormal event will trigger a ticket in ADP's case management system and will be tracked until resolution.

F. Security Logging and Monitoring

[12.4.1] Event logging

[12.4.3] Administrator and operator logs

ADP has implemented a central and read-only logging infrastructure (SIEM) and a log correlation and alerting system (TPSI). Log alerts are monitored and treated in a timely manner by the CIRC.

Such logs include, but are not limited to:

- IDS
- Firewalls
- DNS
- LDAP
- Active Directory
- Operating System
- Internet accesses
- SMTP Gateways

All of these systems are synchronized using a unique NTP based clock reference.

Every single log contains at a minimum:

- Timestamp
- Who (identity of the operator or administrator)
- What (information about the event)

Audit trails and System logging for ADP applications have been designed and set up in order to track the following information:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Systems alerts or failures
- Changes to systems security settings, when the system allows such logging

These logs are only available to ADP authorized personnel, and are sent in live mode to prevent data from being tampered with before being stored in the secure logging appliances.

G. Infrastructure Systems and Monitoring

[12.4.1] Event logging

ADP uses appropriate measures to provide infrastructure monitoring 24 hours per day, 7 days per week. Disruption alerts are managed by different teams according to their severity level and the skills required to resolve them.

ADP hosting center facilities employ monitoring applications that are constantly running on all related processing systems and on the network components to provide ADP staff proactive notification of issues and warnings in anticipation of possible problems. These application functions include, but are not limited to, the following:

- Monitoring and analysis of web site traffic
- Monitoring network equipment

- Monitoring and management of Internet circuit performance and availability
- Monitoring IDS sensors and firewalls for intrusions

H. Technical Vulnerability Management

[12.6.1] Management of technical vulnerabilities

All computers installed in the hosting infrastructure must comply with the installation of a specialized security hardened operating system (or secure build process). Hosted operations employ a hardened, approved and standardized build for every type of server used within our infrastructure. Out-of-the-box installation of operating systems is prohibited since these installations may create vulnerabilities, such as generic system account passwords, that would introduce an infrastructure risk. These configurations reduce the exposure of hosted computers running unnecessary services that can lead to vulnerabilities.

PTSS is responsible for managing the entire assessment and remediation processes. PTSS is independent and maintains a separation of duties from other teams that are responsible for participating in the process, requesting services, and providing remediation efforts.

ADP has developed a documented methodology for conducting release and periodic vulnerability assessments and compliance reviews of Internet facing web-based applications and their corresponding infrastructure components, which include at least 15 primary categories of testing.

Assessment methodology is based on both internal and industry best practices, including, but not limited to, Open Web Application Security Project (OWASP), SANS Institute and Web Application Security Consortium (WASC).

9. Communications Security

A. Network Security Management

[13.1.1] Network controls

[13.1.2] Security of network services

ADP employs a network-based intrusion detection system that monitors traffic at the network infrastructure level (24 hours a day, 7 days a week) and identifies suspicious activity or potential attacks.

ADP only permits modem usage under special, duly justified circumstances and that usage is limited to dial out. Wireless network and access points must be approved by security and are only permitted when configured using secure protocols.

ADP has defined a network management policy and related controls:

a) *Security parameter changes documentation and authorization*: Security parameter change requests (like firewall rule sets) are documented, qualified and authorized by the network competency center prior to being applied into the production environment.

b) *Firewalls facilities and DMZ protections*: ADP network access points are protected by firewalls facilities and Demilitarized Zones (DMZ).

c) *Segregation of network segments*: Production network segments are logically segregated from the end-user network and between environments with different security level.

d) *Relay servers*: Access to systems (network components, application and database servers) is only permitted from authorized relay servers or authentication DMZ.

e) *Data transmission security between ADP data center/infrastructure and its clients*: External data transmissions between ADP data center and its clients are secured via one of the following network means: private leased line, IPSec VPN, MPLS-VPN. Web applications use ADP-approved encryption technology to secure data transmitted by clients to ADP data centers.

Additionally, the GETS Network competency center has implemented a firewall compliance tool. Firewall flows are subjected to change management process before being implemented.

B. Exchange of Information

[13.2.1] Information transfer policies and procedures

ADP implements appropriate controls so that ADP clients' information sent to third parties is transferred between authorized information systems and resources only, and is only exchanged through ADP’s secure and authorized transfer mechanisms.

C. Use of Messaging Systems

[13.2.3] Electronic messaging

ADP prohibits the use of non-secured external instant messaging applications for transmission of client data.

10. System acquisition, development, and maintenance

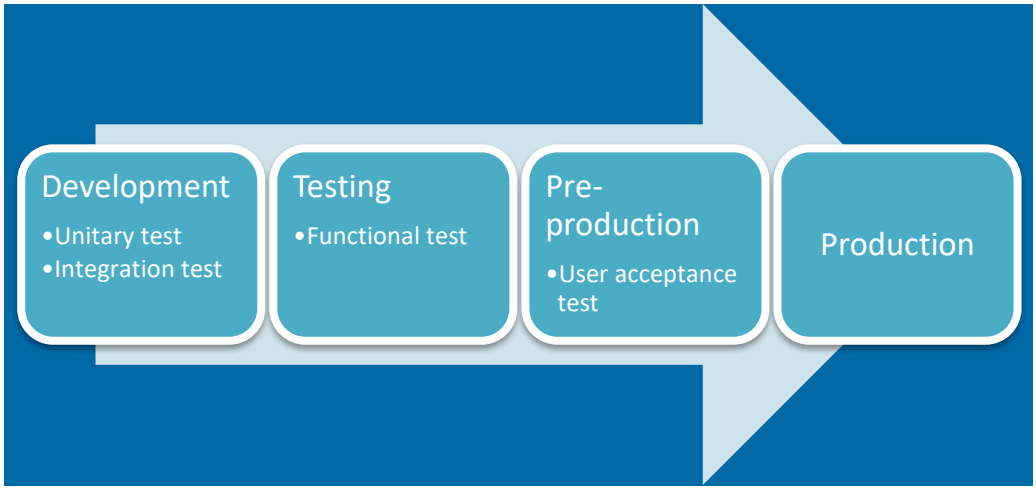
A. Security in Development and Support Processes

[14.1.1] Information security requirements analysis and specification

[14.2.1] Secure development policy

[14.2.2] System change control procedures

During the development cycle, applicable documentation is generated and testing plans are built for the testing phase. Different stages are defined for each environment with relevant approval at each phase:



- From testing to pre-production environment, approval from ADP's Quality team is needed.
- From pre-production to production, approval from IT Operations is required.

Development teams are required to utilize secure coding methods. Application changes are tested in development and regression environments before they reach the production systems. Tests are performed and documented. Upon approval, changes are deployed into production. Penetration testing is performed after siginificant changes.

A periodic CAB, including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place on a regular basis, and are meant to discuss impacts, to agree on deployment windows and to approve the promotion of software packages to production, as well as to inform about any other changes in production infrastructure.

ADP's IT Operations team provides the final approval before any promotion to production environment of the software packages.

B. Security in Development Environment

[14.2.6] Secure development environment

All environments are logically segregated and independent from each other. Software packages are accessible at each stage of the development process and only by the teams involved in that particular stage.

C. Test Data

[14.3.1] Protection of test data

Use of real or unsanitized data in development and testing is not permitted as per ADP's global security policy unless explicitly requested and authorized by client.

11. Supplier relationships

A. Identification of Risks Related to External Parties

[15.1.1] Information security policy for supplier relationships

Risk assessments of third parties who require access to ADP and/or client information are periodically performed with a view to determine their compliance with ADP security requirements for third parties, and to identify any gaps in the applied controls. If a security gap is identified, new controls are agreed upon with such external parties.

B. Information Security Agreements with External Parties

[15.1.2] Addressing security within supplier agreements

ADP enters into agreements with all third parties which include appropriate security commitments in order to meet ADP's security requirements.

12. Information Security Incident Management

A. Management of Information Security Incidents and Improvements

[16.1.1] Responsibilities and procedures

[16.1.4] Assessment of and decision on information security events

ADP has developed a documented methodology for responding to security incidents quickly, consistently, and effectively.

Should an incident occur, a predefined team of ADP employees will activate a formal incident response plan that addresses areas such as:

- Escalations based on the classification of incident or incident severity
- Contact list for incident reporting/escalation
- Guidelines for initial responses and follow up with involved clients
- Compliance with applicable security breach notification laws
- Investigation log
- System recovery
- Issue resolution, reporting, and review
- Lessons learned

ADP policies define a security incident, incident management and all employees' responsibilities regarding the reporting of security incidents. All ADP employees and contractors must read and follow these policies.

ADP also schedules regular training for ADP employees and contractors to ensure awareness of reporting requirements.

13. Information Security Aspects of Business Resiliency Management

A. ADP Business Resiliency Program

[17.1.1] Planning information security continuity

One of ADP's priorities is to establish, maintain and test comprehensive business resumption and contingency planning programs. These programs must allow for the timely and effective recovery of mission-critical ADP business functions in the event of a partial or total loss, preventing an extended period of disruption to any ADP client or ADP business unit.

ADP's Executive Management is committed to protecting ADP's business operations from disruption, ensuring that:

- An understanding of the benefits and goals of the Business Resiliency Program are defined and a proactive approach is taken to Business Resiliency;
- Formal procedures are established to manage business disruptions;
- Business Resiliency requirements are included and implemented in business operations;
- Business Resiliency concepts and controls are understood by associates responsible for responding to incidents and business disruptions;
- Resource requirements are estimated to resume business operations including staffing, facilities, technical infrastructure, information, external services and suppliers and proper resources are allocated to the Business Resiliency Program.

ADP Business Resiliency Organization has documented the Business Resiliency responsibilities of the organization based on Management directives. Among other responsibilities, the ADP Business Resiliency Organization is in charge of:

- Maintaining the Business Resiliency Policy, Standards, Practices and Guidelines for the organization, including the review of these documents on a periodic basis;
- Establishing common systems designated to be used for Plan documentation and notification/escalation processes;
- Maintaining the Business Resiliency Program, including regular reviews, audits, updates to documentation and related procedures;
- Establishing metrics for measuring and demonstrating program effectiveness and maturity;

ADP's Business Resiliency Program is composed of three main components:

- Incident Management, which is in charge of major incident management, and preventing them from escalating to a crisis;
- Business Continuity, to develop protocols that ensure the resumption of business operations;
- Disaster Recovery, where operating procedures to address restoration processes are created and maintained for ADP's critical systems;

B. Implementation of Business Resiliency

[17.1.2] Implementing information security continuity

[17.1.3] Verify, review and evaluate information security continuity

The three components of ADP's Business Resiliency Program – Incident Management, Business Continuity, and Disaster Recovery – are deployed following the following phases:

- **Risk Threat Analysis (RTA)**
  The Risk Threat Analysis is used to evaluate threats against all ADP locations worldwide, and rate this risk in order to assign a risk level to each facility. It is required to be reviewed periodically or sooner if a significant event has occurred.

- **Business Impact Analysis (BIA)**
  A formal Business Impact Analysis has been conducted and is regularly reviewed to identify critical business processes that need to be recovered after a business disruption. The BIA is required to be reviewed and revised periodically or sooner if a significant event or a change in a critical business function has occurred. The Business Impact Analysis identifies:
  - Critical business functions and processes;
  - IT applications that support the identified critical business functions;
  - Interdependencies of processes, assets, infrastructure and resources;
  - Recovery Time Objectives (RTO's) and Recovery Point Objectives (RPO's) for processes and data;
  - Estimated potential losses from a business disruption.

- **Incident Management and Business Continuity Plans Development**
  Once the RTA and BIA are completed, all information is compiled and Incident Management Plans and Business Continuity Plans are created.

  ADP has defined this set of plans and capabilities that work together collectively to enhance the ADP Business Resiliency Program thereby minimizing the adverse impacts a disruption may have on ADP service delivery to clients and third parties.

- **Testing and Exercising**
  Business Resiliency Plans are tested periodically through a table-top exercise held with the Crisis Committee. This exercise is limited to a basic scenario and a theoretical discussion, testing the abilities and reaction capabilities of the Incident Management Committee.

- **Maintenance**
  The overall Business Resiliency Program is reviewed and revised at least once annually or more frequently as required due to changes in personnel or other circumstances. Additionally, various components may be subject to periodic reviews.

C. Availability of Disaster Recovery Facilities

[17.2.1] Availability of information Processing facilities

[10.5] Back-Up

In addition, a standard Disaster Recovery operating procedure contains detailed plans to address restoration processes for ADP's mission critical systems, based on the following scenarios:

- Critical equipment failure at the primary computing center
- Site disaster at the primary computing center

ADP data is synchronized on an ongoing basis between the primary Data Center and the disaster recovery site. Local back-ups are also stored in the primary Data Center in order to keep a longer period and volume of data.

The IT department conducts an annual test of its ability to restore the IT platforms and communication capabilities, which support the critical business functions. Business units define and validate the DRP test scope together with GETS. Once the DRP scope is defined and validated, several teams from the IT department and business units are involved.

The Disaster Recovery test methodology covers the following areas:

- Disaster Recovery Plan Playbook: technical documentation to activate the DRP;
- Disaster Recovery testing: technical and functional test scripts to validate DRP activation;
- Disaster Recovery test results: executive report, including results of the DRP test as well as findings and lessons learned;
- Disaster Recovery improvement activities: post mortem review action items and plan.

Guidelines describing preparatory measures and communication plans in case of a severe incident are published and communicated to all employees and relevant external parties, in order to be prepared. These include:

- Internal and external communication guidelines;
- Preparatory guidelines and preventive measures for employees;
- Planned or unplanned building evacuation simulation, updated annually.

14. Compliance

A. Compliance with Legal Requirements

[18.1.1] Identification of applicable legislation and contractual requirements

ADP privacy and security controls are designed to allow us to meet the obligations imposed on data processors by data protection laws in all of the countries where ADP offers its services, including those deriving from the Data Protection Directive 95/46/EC and EU's Global Data Protection Regulation (officially, Regulation (EU) 2016/679) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ADP reserves the right to use third party data processors and subcontractors including for processing, hosting and storage purposes. ADP remains responsible for the quality of the services and for these sub-processors' compliance with data protection / privacy law as it applies to data processors. ADP is committed to working with its clients to achieve an appropriate level of transparency around its use of sub-processors.

In order to protect its clients' personal data (client information) wherever they are processed, ADP has implemented a Global Privacy Policy that provides the foundation for the processing of client data worldwide. The Global Privacy Policy requires every ADP affiliate and every ADP associate to protect client personal data and to only use it for the purposes specified in our client contracts.

B. Compliance with Security Policies and Standards

[18.2.1] Independent review of information security

[18.2.3] Technical compliance review

To the extent indicated in the terms and conditions of the Agreement, ADP performs a SOC1[2] type II audit on a periodic basis. These audits are conducted by a well-known third-party audit firm and audit reports are available on a yearly basis for clients upon request, when applicable.

C. Technical Compliance

[18.2.2] Compliance with security policies and standards

In order to ensure technical compliance with best practices, ADP performs regularly scheduled network vulnerability scans. The scan results are then prioritized and developed into corrective action plans with the hosting teams and their management.

Vulnerability scans are performed on a product-by-product basis. Utilizing specialized application scanning tools, application level vulnerabilities, if any, are identified, shared with the product development management teams, and incorporated into the quality assurance processes for corrective action. The results are analyzed and corrective action plans developed and prioritized.

[2] In the case of certain US Services offered by ADP, there would be also SOC 2 Type II exec. reports

D. Retention of Data

[18.1.3] Protection of records

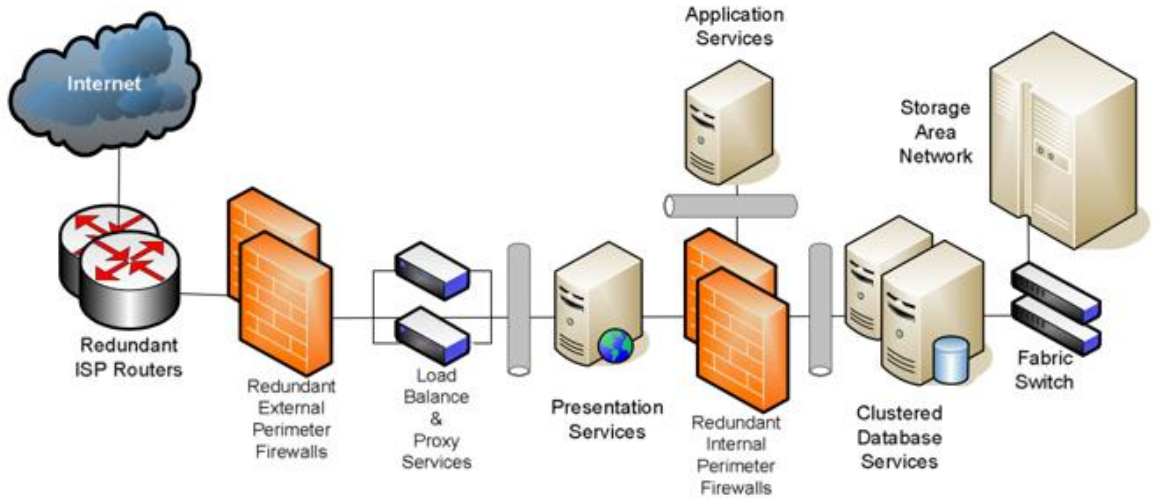
ADP's data retention policy regarding client information is designed to comply with applicable laws.

At the end of a client contract, ADP will comply with its contractual obligations relating to client's information, i.e. ADP will either return, or allow client to retrieve (e.g. by data download), all client information required for the continuity of client's business activities (if not previously provided). Then ADP will securely destroy remaining client information, except to the extent required under applicable law, authorized by the client or needed for dispute resolution purposes.

15. Appendix

A. Logical Network Diagram

The illustration below provides a logical representation of our approach:



ANNEX 3 – List of Group Companies bound by Processor Code

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 Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
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 GmbH	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 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 Gestion des Paiements 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 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 B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Netherlands
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 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, LLC	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 Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ
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