CERIDIAN

DATA PROCESSING ADDENDUM

This Data Processing Addendum and its annexes set forth the terms and conditions pursuant to which Personal Data will be transferred and processed in the framework of the Agreement.

DEFINITIONS

For the purposes of this Data Processing Addendum, capitalized terms used shall have the following meanings:

"Authentication Credentials"	means the mechanism/tool used to prove a person's identity, such as passwords and access tokens.
"Controller"	means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
"Data Protection Legislation"	means, the applicable Laws of any country with regard to the protection of Personal Data relating to the Services, as amended or replaced from time to time, including where applicable: (i) until 24 May 2018, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the transposition thereof in the relevant national legislation, and (ii) as from 25 May 2018, EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**General Data Protection Regulation**" or "**GDPR**") (i and ii together "**EU Data Protection Laws**") .
"Data Subject"	means an identified or identifiable natural person to whom the Personal Data relates. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The relevant categories of Data Subjects are identified in ***ANNEX 1***.
"Law(s)"	means all laws or statutes of any jurisdiction and any other regulation, ordinance, order, decree or rule having the force of law, whether in existence as of the Effective Date or promulgated thereafter, as amended or superseded, to the explicit exclusion of Client-specific legal sources.
"Personal Data"	means any information relating to a Data Subject. The relevant categories of Personal Data that are provided to Ceridian by, or on behalf of, Client are identified in ***ANNEX 1***.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the provisioning of the Services.
"Privacy Contact Person"	means the individual(s) assigned in Article 10 by a Party and communicated to the other Party as point of contact and representing the Party for (a part of) the Services.
"Processing", "Process(es)" or "Processed"	means any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Processor"	means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller.
"Standard Contractual Clauses"	means the standard contractual clauses of which the European Commission on the basis of Article 26 (4) of Directive 95/46/EC decided that these offer sufficient safeguards for the transfers of personal data to a third country, or the data protection clauses adopted by the European Commission or by a supervisory authority and approved by the European Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR. Data protection clauses adopted in accordance with the GDPR shall replace and prevail over any standard contractual clauses adopted on the basis of Directive 95/46/EC to the extent that they intend to cover the same kind of data transfer relationship.
"Sub-processor"	means any Ceridian Contractor who agrees to receive Personal Data intended for Processing.

ARTICLE 1 INTERPRETATION

1.1 This Data Processing Addendum forms an integral part of the Agreement. The provisions of the Agreement therefore apply to this Data Processing Addendum. All capitalized terms not defined in this Data Processing Addendum will have the meaning set forth in the Agreement.

1.2 This Data Processing Addendum constitutes the entire agreement and understanding between the Parties in respect of the subject matter hereof and supersedes, cancels and nullifies any previous provisions agreed between the Parties in relation to such subject matter.

ARTICLE 2 SPECIFICATION OF THE DATA PROCESSING

2.1 Any Processing of Personal Data under the Agreement shall be performed in accordance with the applicable Data Protection Legislation. However, Ceridian is not responsible for compliance with any Data Protection Legislation or other Laws applicable to Client or Client's industry that are not generally applicable to Ceridian as a service provider.

2.2 For the performance of the Services, Ceridian is a Processor acting on behalf of the Controller, in particular Client or as the case may be Client's Affiliate(s). Client warrants and represents that it is and will at all times remain duly and effectively authorized to give the instructions set out in this the Agreement on behalf of each Affiliate (who may be, as the case may be, the actual Controller for the processing of Personal Data). As a Processor, Ceridian will only act upon Client's instructions (for the purpose of the Agreement, acting on its own behalf and on behalf of its Affiliate(s)). The following is deemed an instruction to Ceridian to Process Personal Data: (a) Processing in accordance with the Agreement (b) Processing initiated by Client users in their use of the Services.

2.3 A more detailed description of the subject matter of the Processing of Personal Data in terms of the concerned categories of Personal Data and of Data Subjects and of the instructions and purposes for the Processing of Personal Data is contained in ***ANNEX 1*** hereto and in the Agreement.

2.4 Ceridian may direct to Client any requests of Data Subjects, Personal Data Breach notifications, requests for audit or investigation or any other requests. Client shall subsequently internally distribute such request or notifications to any other relevant Controller, and Ceridian reserves the right to direct any such requests and notifications to any other relevant Controller directly.

ARTICLE 3 DATA SUBJECTS' RIGHTS

3.1 With regard to the protection of Data Subjects' rights pursuant to applicable Data Protection Legislation, Client shall facilitate the exercise of Data Subject rights and shall ensure that adequate information is provided to Data Subjects about the Processing hereunder in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

3.2 Should a Data Subject directly contact Ceridian wanting to exercise his or her individual rights such as requesting a copy, correction or deletion of his or her data or wanting to restrict or object to the Processing activities, Ceridian will direct such Data Subject to Client. In support of the above, Ceridian may provide Client's basic contact information to the requestor, and, to the extent disclosed by Data Subject, Data Subject's basic contact information and a summary of the request to Client. Client shall inform Data Subjects that they may exercise these rights solely vis-à-vis Client. Client agrees to answer to and comply with any such request of a Data Subject in line with the provisions of the applicable Data Protection Legislation.

3.3 Ceridian shall use commercially reasonable efforts to cooperate with and assist Client for the fulfilment of Client's obligations under applicable Data Protection Legislation to respond to requests from Data Subjects exercising their rights.

ARTICLE 4 CONSULTATION AND CORRECTION OF PERSONAL DATA

4.1 Where Personal Data is not made available through self-service access to Client or Client's employees, Ceridian will, within a reasonable period of time, as necessary under the applicable Data Protection Legislation and upon payment of a fee on a time and materials basis at Ceridian's then current rates, either: (a) provide Client, in its role of Controller, with the ability to consult or correct Personal Data; or (b) provide Client with a copy of the Personal Data that it Processes and make any corrections on Client's behalf in accordance with the instructions of Client.

ARTICLE 5 DISCLOSURE

5.1 Ceridian will not disclose Personal Data to any third party, except (a) as Client directs, (b) as stipulated in the Agreement (c) as required for Processing by approved Sub-processors in accordance with Article 10 or (d) as required by Law.

5.2 Ceridian shall inform the persons acting on its behalf and having access to Personal Data about the applicable requirements and ensure their compliance with such requirements through contractual or statutory confidentiality obligations to maintain the security and confidentiality of Personal Data in accordance with provisions appropriate to the sensitivity of the Personal Data.

ARTICLE 6 DELETION AND RETURN OF PERSONAL DATA

6.1 Client Data:

(a) Upon termination of the Agreement, Ceridian shall delete Personal Data on its systems (without prejudice to any backup archives) unless otherwise instructed by Client prior to the effective date of termination. Ceridian shall cooperate reasonably and in a timely manner with the efforts by Client, or any other party acting on Client's behalf, to provide for an orderly transition of the applicable Services to Client or another service provider. The costs attached to such request are at Client's expense.

(b) During the Service Term, Ceridian may make available, for some products, limited purge functionality. Ceridian is not responsible for compliance with Client's data retention requirements.

6.2 Ceridian Data: Notwithstanding anything to the contrary, Ceridian may retain or dispose of Ceridian records that may contain Client Data only for as long as there exists a legitimate business purpose or legal requirement to do but in compliance with applicable Data Protection Legislation and subject to the protections of this Data Processing Addendum.

ARTICLE 7 LOCATION OF PROCESSING

7.1 Personal Data that Ceridian processes on Client's behalf may be Processed in any country in which Ceridian, its Affiliates and authorized Sub-Processors maintain facilities to perform the Services and Client authorizes Ceridian to perform any such transfer of Personal Data to any such country and to Process Personal Data in such country in relation to the provision of the Services. Any transfer from one territorial jurisdiction to another territorial jurisdiction (the EU constituting one single jurisdiction for the purpose of this Article) will only be undertaken in compliance with the applicable Data Protection Legislation, such as the execution of an additional data processing addendum (an "Onward Transfer Addendum").

ARTICLE 8 USE OF SUB-PROCESSORS

8.1 Client acknowledges and expressly agrees that Ceridian may transfer Personal Data to third party Sub-processors for the provision of the Services if such transfer is done in accordance with the terms of this Article 8.1.

8.2 Ceridian will enter into written agreements with any such Sub-processor which contain data protection obligations appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, taking also into account the state of technology and the cost of their implementation, including where applicable, an Onward Transfer Addendum. Client hereby explicitly grants Ceridian a mandate to execute and enforce the Standard Contractual Clauses on its behalf against Ceridian's relevant Sub-processors, such an Onward Transfer Addendum being governed by the present Data Processing Addendum. Sub-processor written agreements will permit Sub-processors to obtain Personal Data only to deliver the services Ceridian has entrusted them with and will prohibit Sub-processors from using such Personal Data for any other purpose.

8.3 Where required by the GDPR, Ceridian will make available a list of Sub-processors and will provide a notice mechanism to inform Client about changes relating to the Sub-processors. This notice mechanism represents Ceridian's duty to inform and request consent from Client for the use of a new Sub-processor.

(a) If Client reasonably objects to the Processing of Personal Data by one or more Sub-processors, then Client shall notify Ceridian in writing (including e-mail) within fourteen (14) Business Days after receipt of Ceridian's notice.

(b) In the event Client objects to a Sub-processor, Ceridian will use reasonable efforts to change the affected Services or to recommend another commercially reasonable change to Client's use of the affected Services to avoid the Processing of Personal Data by the Sub-processor concerned. If Ceridian is unable to make available or propose such change within (60) calendar days, Client may terminate the relevant part of the Agreement regarding those Services which cannot be provided by Ceridian without the use of the Sub-processor concerned as its sole and absolute remedy. To that end, Client shall provide written notice of termination taking into account a notice period of 6 months and providing a reasonable motivation for non-approval.

ARTICLE 9 TECHNICAL AND ORGANIZATIONAL MEASURES

9.1 Ceridian has implemented and will maintain a security program that takes into account appropriate technical and organizational measures appropriate to the nature and sensitivity to the data, intended to protect Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. This program shall address the following:

(a) the prevention of unauthorized persons from gaining physical access to systems Processing Personal Data (physical access control);

(b) the prevention of systems Processing Personal Data from being used without authorization (logical access control);

(c) ensuring that persons entitled to use a system Processing Personal Data gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);

(d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);

(e) ensuring the establishment of an audit trail to document whether and by whom Personal Data has been entered into, modified in, or removed from systems Processing Personal Data (entry control);

(f) ensuring that Personal Data Processed is Processed solely in accordance with the instructions (control of instructions);

(g) ensuring that Personal Data is protected against accidental destruction or loss (availability control).

9.2 The present technical and organizational addressed by Ceridian's security program are described in ***ANNEX 2*** of this Data Processing Addendum. Ceridian may adapt such measures from time to time, for example, as a result of the development of regulations, technology and other industry considerations. In any event, the implemented technical and organizational measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, taking also into account the state of technology and the cost of their implementation.

9.3 During the term of this Data Processing Addendum, Client may request Ceridian to provide Client within a reasonable period of time with an updated description of the implemented technical and organizational protection measures.

ARTICLE 10 PRIVACY AND DATA PROTECTION REPRESENTATIVE

10.1 The Parties shall appoint an individual responsible for privacy and data protection matters, including where applicable, a data protection officer.

For Ceridian HCM:
Chief Privacy Officer
Privacy@Ceridian.com
3311 East Old Shakopee Road, Bloomington MN, 55245

10.2 Upon the effective date of this Data Protection Addendum, Client shall notify Ceridian's Privacy Contact Person identified in this Article 10 in writing of the identify of its privacy contact or, if applicable, its data protection officer. In the event Client does not provide a Privacy Contact Person pursuant to this Article 10, Ceridian may use the process for notices set forth in the Agreement.

ARTICLE 11 PERSONAL DATA BREACH

11.1 In the event of a Personal Data Breach and irrespective of its cause, Ceridian shall notify Client without undue delay after having become aware of such Personal Data Breach, specifying where known or readily identifiable:

(a) the nature of the Personal Data Breach;
(b) the categories and approximate number of Data Subjects and Personal Data records concerned;
(c) as the case may be, the remedial actions taken or proposed to be taken to address the Personal Data Breach, to mitigate its effects and to prevent recurrence;
(d) the identity and contact details of the data protection officer or the Privacy Contact Person from whom more information can be obtained.

11.2 Client must notify Ceridian promptly about any possible misuse of its accounts or Authentication Credentials or any security issue related to its use of the Services.

11.3 The Party responsible for the Personal Data Breach shall without undue delay further investigate the Personal Data Breach and shall keep the other Party informed of the progress of the investigation and take reasonable steps to further minimize the impact. Both Parties agree to fully cooperate with such investigation and to assist each other in complying with any notification requirements and procedures.

11.4 A Party's obligation to report or respond to a Personal Data Breach is not and will not be construed as an acknowledgement by that Party of any fault or liability with respect to the Personal Data Breach.

11.5 To the extent that a Personal Data Breach is determined to be a result of Ceridian's breach of this Data Processing Addendum, Ceridian shall, at Ceridian's cost, undertake to the extent reasonable and appropriate under the circumstances (a) notify public authorities, individuals, or other required persons, and/or (b) provide one year of credit monitoring services. The timing, content, and manner of any notices shall be determined by Client in its sole discretion provided Ceridian shall have a right to review and approve any statements referencing Ceridian. Ceridian shall not be responsible for failure of any notice to comply with applicable Law or other damages that result from remedial actions to the extent such actions were requested or directed by Client. Ceridian and Client will jointly cooperate to determine the need for and scope and nature of any credit monitoring to ensure such monitoring is sufficient to mitigate any reasonably anticipated financial harm.

ARTICLE 12 DATA PROTECTION IMPACT ASSESSMENTS

12.1 Where Client is obligated by applicable Data Protection Legislation to execute a data protection impact assessment ("DPIA"), Ceridian shall provide reasonable cooperation and assistance to Client for the execution of the DPIA to allow Client to comply with its obligations. Ceridian shall be entitled to invoice Client on a time and material basis at the Ceridian's then current rates for any time expended for any such assistance.

ARTICLE 13 CLIENT RESPONSIBILITIES

13.1 Client shall comply with the applicable Data Protection Legislation as well as any other Laws applicable to Client or Client's industry. If compliance with any such specific Laws requires any actions with regard to data protection on the part of Ceridian in addition to the obligations set forth in this Data Processing Addendum, such actions will only be taken upon mutual agreement between the Parties. For the avoidance of doubt, Ceridian will use commercially reasonable efforts to accommodate additional requirements, but shall not be obligated to do so. In any event, Client will provide reasonable advance notice of the required actions, cooperate fully with Ceridian in respect thereof and compensate Ceridian for any such efforts that require additional services or investment or modifications in the Services.

13.2 Client is solely responsible for the lawfulness of Personal Data and the Processing thereof under the Agreement.

13.3 Client represents and warrants that, where it provides any Personal Data to Ceridian for Processing by Ceridian:

(a) it has duly informed the relevant Data Subjects of their rights and obligations, and in particular has informed them of the possibility of Ceridian (or a category of service providers to which Ceridian belongs) Processing their Personal Data on Client's behalf and in accordance with its instructions;
(b) it has complied with all applicable Data Protection Legislation in the collection and provision to Ceridian of such Personal Data;
(c) the Processing of such Personal Data in accordance with the instructions of the Controller is lawful.

13.4 Client shall take reasonable steps to keep Personal Data up to date to ensure the data are not inaccurate or incomplete with regard to the purposes for which they are collected.

13.5 With regard to components that Client provides or controls, including but not limited to workstations connecting to Ceridian Services, data transfer mechanisms used and credentials issued to Client personnel, Client shall implement and maintain the required technical and organizational measures for data protection.

ARTICLE 14 NOTIFICATIONS

14.1 Unless legally prohibited from doing so, Ceridian shall notify Client as soon as reasonably possible if it or any of its Sub-processors, with regard to Client's Personal Data:

(a) receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing;
(b) intends to disclose Personal Data to any competent public authority outside the scope of the Services of the Agreement. At the request of Client, Ceridian shall provide a copy of the documents delivered to the competent authority to Client.

14.2 Any notification under this Data Processing Addendum, including a Personal Data Breach notification, will be delivered to one or more of Client's Privacy Contact Persons via e-mail. Upon request of Client, Ceridian shall provide Client with an overview of the contact information of the registered Client's Privacy Contact Persons. It is Client's sole responsibility to timely report any changes in contact information and to ensure Client's Privacy Contact Persons maintain accurate contact information.

ARTICLE 15 AUDIT & COMPLIANCE

15.1 In addition to Ceridian's obligations in Article 9.3, where required by applicable Data Protection Legislation, Ceridian will assist Client in demonstrating compliance with this Data Protection Addendum by making available upon request of Client information reasonably necessary to demonstrate such compliance. Ceridian will notify Client if Ceridian receives an instruction that infringes the Data Protection Legislation and/or the obligations of this Data Processing Addendum during the course of the inspection by Client or its authorized third party.

15.2 Where required by applicable Data Protection Legislation, or where a competent data protection authority requires this under applicable Data Protection Legislation. Client may, upon thirty (30) calendar days' prior written notice, at its own expense, instruct acknowledged audit professionals to conduct an audit of Ceridian's compliance with applicable Data Protection Legislation once every twelve (12) months provided that such additional audit inquiries shall not unreasonably impact in an adverse manner Ceridian's regular operations and do not prove to be incompatible with the applicable legislation or with the instructions of a competent authority;

15.3 Before the commencement of any such additional audit inquiries, Client and Ceridian shall mutually agree upon the scope, timing and duration of the audit.

15.4 Client shall promptly notify Ceridian with information regarding any non-compliance discovered during the course of additional audit inquiries. Client agrees to provide Ceridian with a draft of the audit report for review. Ceridian is entitled to propose any amendments and add management comments to this draft before Client establishes the final version.

15.5 During such audit, Ceridian shall provide reasonable cooperation and assistance to the auditors. Ceridian shall be entitled to invoice Client on a time and material basis at Ceridian's then current rates for any time expended for any such audit inquiries. Client shall not be entitled to claim compensation for any kind of audit expenses incurred by Client.

15.6 The Ceridian audit report, any other information to which Client or the aforementioned audit professionals have access pursuant to any audit activities, as well as an attestation of the implementation of the technical and organizational measures to protect Personal Data will be considered Ceridian Confidential Information.

ARTICLE 16 TERM AND TERMINATION

16.1 This Data Processing Addendum comes into effect on the date noted above, and remains in force until Processing of Personal Data by Ceridian is no longer required (a) in the framework of or pursuant to the Agreement or (b) for a period after termination of the Agreement or the relevant Services for any reason whatsoever, in accordance with Client's explicit instructions or other legally permissible basis.

ARTICLE 17 APPLICABLE LAW

17.1 This Data Processing Addendum and any rights and obligations arising out of it shall be interpreted according to and governed by the law governing the Agreement.

ANNEXES

1. Details of the Personal Data Processing
2. Technical and Organizational measures

ANNEX 1: DETAILS OF THE PERSONAL DATA PROCESSING

ARTICLE 1 DATA SUBJECTS

Present and former job candidates, employees, contractors, agents and other collaborators of Client, as well as third parties who are appointed by the aforementioned persons as family members or contact persons.

ARTICLE 2 CATEGORIES OF PERSONAL DATA

The Personal Data transferred concerns all relevant information that is required to deliver the requested Services, which may include (a subset of) the following categories of data:

(a) Personal details such as name, birth date, etc.
(b) Contact details such as address, e-mail address, telephone number, etc.
(c) Marital status and information on partner and children
(d) Payment details, including bank account number
(e) Employee number
(f) Job (description)
(g) Employee contract data including but not limited to gross salary, compensations and other employee benefits
(h) Social security number (if required for government declarations), such as Rijksregisternummer (INSZ) in Belgium or Burgerservicenummer (BSN) in the Netherlands
(i) Expenses
(j) Time registration and absence information
(k) Qualifications, including CV and references
(l) Information regarding education, training, etc. the Data Subject has received or will follow
(m) Information regarding personal development and evaluations
(n) Authentication Credentials to use the Services, such as username, IP address, PC Name, etc.
(o) Activities performed by Client users in their use of the Services
(p) Any other category of Personal Data agreed upon between Parties in the relevant service exhibit, service particulars, order form, statement of work or any other document of the Agreement.

Client's data fields can be partly configured as part of the implementation of the Services or as otherwise permitted within the scope of the Services.

ARTICLE 3 PURPOSES OF PROCESSING OF PERSONAL DATA

Personal Data will be Processed for the following purposes:

(a) performance of the Services including but not limited to:
  i) Employee HR administration
  ii) Payroll and employee benefits administration
  iii) Compliance with social and fiscal Laws
  iv) Management of employee development and training plans
  v) Personal development and performance evaluation of employees
  vi) Work planning and organization
(b) Benchmarking and analytics
(c) Providing access to information systems and premises
(d) Continuous improvement and development of products, services and software
(e) Compliance with Data Protection Legislation and information security requirements
(f) Managing Ceridian's business operations, for example, claims management with and between Client, Ceridian, the Data Subject(s) and/or third parties, including beyond termination of the Agreement for any reason whatsoever
(g) Any other purpose of Processing of Personal Data agreed upon between Parties in the relevant service exhibit, service particulars, order form, statement of work or any other document of the Agreement.

For the avoidance of doubt, Personal Data will be Processed beyond termination of the Agreement for the purposes established in (b), (d), (e), (f), and (g).

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Domain	Practices
Information Security Policy and Organization of Information Security	**Ownership for Security and Data Protection**. Ceridian has appointed an Information Security Officer responsible for coordinating and monitoring the security rules and procedures as well as data protection compliance. **Security Roles and Responsibilities**. Security responsibilities of Ceridian co-workers are formally documented and published in security and privacy policies. **Risk Management Program**. Ceridian executes periodical risk assessments of the implemented security controls.
Human Resources Security	**Confidentiality obligations**. Ceridian co-workers are subject to written confidentiality obligations **Security and privacy training**. Ceridian informs its co-workers about relevant security measures to protect Personal Data. **Termination.** Ceridian ensures according to formal security administration procedures that access rights are timely revoked upon termination.
Asset Management	**Asset Inventory**. Ceridian maintains an inventory of all computing equipment and media used. Access to the inventories is restricted to authorized Ceridian personnel. **Asset Handling** • Personal Data on portable devices are encrypted. • Ceridian has procedures for securely disposing of media and printed materials that contain confidential data.
Cryptography	Encryption of Personal Data is performed according to formal processes and encryption standards. Encryption mechanisms follow the highest standards available, only using strong ciphers.
Physical and Environmental Security	**Physical Access to Facilities**. • Ceridian limits access to facilities where Personal Data are processed to identified and authorized individuals. • Physical access to data centers is only granted following a formal authorization procedure and access rights are reviewed periodically **Protection from Disruptions**. Ceridian uses a variety of industry standard systems to protect its data centers against loss of data due to power supply failure, fire and other natural hazards.
Access Control	**Access Policy**. Ceridian enforces an access control policy based on least privileges principles. **Access Authorization** • Ceridian has implemented and maintains an authorization management system that controls access to systems containing Personal Data. • Every individual accessing systems containing Personal Data has a separate, unique identifier/username. • Ceridian restricts access to Personal Data to those individuals who require such access to perform their job function. **Authentication** • Ceridian uses industry standard practices to identify and authenticate Users who attempt to access Ceridian network or information systems, including strong authentication. • Where Authentication Credentials are based on passwords, Ceridian requires that the passwords are at least eight characters long and sufficiently complex. • De-activated or expired identifiers/usernames are not granted to other individuals. • Accounts will be locked out in case of repeated attempts to gain access to the information system using an invalid password. • Ceridian maintains practices designed to ensure the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network access**. Ceridian maintains control measures (e.g. firewalls, security appliances, network segmentation) to provide reasonable assurance that access from and to its networks is appropriately controlled.
Operations Security	**Data Recovery Procedures** • On an ongoing basis, but in no case less frequently than once a day (unless no data has been updated during that period), Ceridian maintains backup copies of Personal Data for recovery purposes. • Ceridian stores copies of Personal Data and data recovery procedures in a different place from where the primary computer equipment processing the Personal Data is located. **Malicious Software**. Ceridian maintains anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data. **Security updates**. Security patches are installed following a documented security patch management process. **Event Logging**. Ceridian logs access and use of its information systems containing Personal Data, registering the access ID, time and relevant activity.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Domain	Practices
Communications Security	**Network Segregation**. Ceridian has implemented a network segmentation policy and controls to avoid individuals gaining access to communication and systems for which they have not been authorized. **Transfer outside own network**. Ceridian encrypts, or provides the mechanisms to Client to encrypt, Client information that is transferred across public networks. **Information Transfer**. Any transfer of Personal Data to third parties is only performed when authorized and following the execution of a formal written non-disclosure agreement.
System Acquisition, Development & Maintenance	**Security Requirements**. Requirements for protecting data and systems are analyzed and specified. **Change Control**. Ceridian has implemented a formal change management process to ensure changes to operational systems and applications are performed in a controlled way.
Supplier Relationships	**Supplier Selection**. Ceridian maintains a selection process by which it evaluates the security and privacy practices of a subcontractor with regard to data handling. **Contractual Obligations**. Suppliers with access to Personal Data are subject to data protection and security obligations and these are formally integrated into supplier contracts.
Information Security Incident Management	**Incident response**. Ceridian maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported. **Incident notification**. For each security breach that impact the confidentiality or integrity of Personal Data, notification by Ceridian will be made without unreasonable delay.
Business Continuity Management	**Disaster Recovery**. Ceridian maintains a disaster recovery program (DRP). **Redundancy**. Ceridian's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its last-replicated state from before the time it was lost or destroyed.
Compliance	**Security Reviews**. Information security controls are independently audited and reported to management on a periodical basis.