dun & bradstreet

Statement of Applicability

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
5 Organizational Controls			
Policies for information security	5.1	Yes	Our Information Security and Privacy Information related policies are approved by management, communicated to, and acknowledged by, relevant interested parties. All policies remain valid until reissued or retired and are reviewed at planned intervals, or sooner if significant changes occur.
Information security roles and responsibilities	5.2	Yes	Responsibility and accountability for the management of global Information Security & Privacy Information reside with our Chief Cyber Security & Technology Risk Officer and our Chief Ethics & Compliance Officer. Responsibility for management of the ISMS & PIMS is delegated to the Director of International Business Operations. Individual leaders are responsible for resourcing and implementing controls as appropriate to their role.
Segregation of duties	5.3	Yes	Conflicting duties and areas of responsibility are segregated.
Management responsibilities	5.4	Yes	Being 'Data Inspired' is one of Dun & Bradstreet's core values and the importance of data and information Security & Privacy is part of the culture of our business. Leaders reinforce that all employees are required to comply with company policies and procedures. Mechanisms are in place to facilitate reporting any instance of noncompliance.
Contact with authorities	5.5	Yes	We maintain contact with relevant law enforcement and regulatory bodies both in the normal course of our business and in exceptional circumstance to report security incidents or to maintain continuity of our business.
Contact with special interest groups	5.6	Yes	We are members of specialist security and privacy related interest groups and forums.
Threat intelligence	5.7	Yes	Information Security threat information is collected and analysed to produce threat intelligence.
Information security in project management	5.8	Yes	Information Security and Privacy Information are considered and tracked as appropriate in all projects.
Inventory of information and other associated assets	5.9	Yes	Inventories of Dun & Bradstreet information assets are maintained on dedicated systems. All information related assets (or groups of assets) have designated owners who are responsible for the asset throughout its lifecycle or owners for defined phases of the asset's lifecycle.
Acceptable use of information and other associated assets	5.10	Yes	Acceptable use of information and assets is defined in our Acceptable Use Policy and is reinforced through training and awareness courses.
Return of assets	5.11	Yes	Procedures are in place to ensure that company assets that are assigned to employees or contractors are returned when the contract with the employee or contractor ends.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Classification of information	5.12	Yes	Information is classified in accordance with our Data Compliance and Ethics Policy and labelled as set out in our policies and standards. They guide asset owners and employees on the appropriate labelling and handling of information assets.
Labelling of information	5.13	Yes	
Information transfer	5.14	Yes	Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities. Security training re-enforces our policies. Agreements are in place between Dun & Bradstreet and 3rd party Vendors and Business Partners. Information involved in electronic messaging is appropriately protected.
Access control	5.15	Yes	Access to facilities, networks and systems is controlled by our policies and standards. User Requests are managed by an online process controlling and limiting access to an as needed basis.
Identity management	5.16	Yes	Identity and Access Management Standard addresses requirements for identity management throughout the lifecycle of the identity.
Authentication information	5.17	Yes	Allocation of authentication information (passwords, private keys/certificates, and tokens) is controlled through a formal management process. Systems for managing passwords are interactive to ensure quality passwords. Training is provided to users and includes: guidance for creating strong passwords and PINS and keeping them confidential; use of MFA; private keys; etc. Vendors and contractors are contractually obliged to maintain confidentiality of information. Where access is granted to third parties it is limited in accordance with our policy.
Access rights	5.18	Yes	There are global policies and standards in place covering user registration; de-registration; granting, provisioning; and revoking access rights to all user types, systems, and services. User access rights are periodically reviewed.
Information security in supplier relationships	5.19	Yes	In our Third-Party Compliance processes, we identify risks associated with engagements with external providers. Through agreements, contracts, and code of conduct, we require our vendors to meet Information Security & Privacy Information requirements as set out in relevant policies.
Addressing information security within supplier agreements	5.20	Yes	Appropriate arrangements are in place in relation to Information Security & Privacy Information agreements with 3rd Party Vendors and Business Partners
Managing information in the ICT supply chain	5.21	Yes	Agreements with Vendors include requirements that address the Information Security & Privacy Information risks associated with information and communication technology services and product supply chain.
Monitoring, review and change management of supplier services	5.22	Yes	Dun & Bradstreet monitors, reviews and audits vendor service delivery, where required. Changes to the provision of services by suppliers is carefully managed.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Information security for use of cloud services	5.23	Yes	The acquisition, use, management, and exit of cloud services is aligned to our Information Security & Privacy Information Management System requirements.
Information security incident management planning and preparation	5.24	Yes	Management responsibilities and procedures are established to ensure a quick, effective, and orderly reporting of and response to Information Security & Privacy Information incidents.
Assessment and decision on information security events	5.25	Yes	The assessment of Information Security & Privacy Information events and the decision to classify as an incident is defined in policy and procedure documents.
Response to information security incidents	5.26	Yes	Coordinated response steps to Information Security & Privacy Information incidents are defined in policy and procedure documents.
Learning from information security incidents	5.27	Yes	Post-incident activities enable us to apply a learning and continual improvement approach to all Information Security & Privacy Information incidents.
Collection of evidence	5.28	Yes	Policy and process set out the procedure for gathering and retaining evidence and the chain of custody.
Information security during disruption	5.29	Yes	A managed process has been developed, and is maintained, for business continuity throughout Dun & Bradstreet and with relevant 3rd Party vendors. It addresses the Information Security & Privacy Information requirements needed for the organization's business continuity, with plans to maintain or restore operations at the required level and in the required timescales following interruption to critical business processes. Business Continuity Plans are tested and updated periodically to ensure that they are up to date and effective.
ICT readiness for business continuity	5.30	Yes	Information and communication technology availability, and readiness to recover, is built into our Business Continuity Management and Disaster Recovery planning.
Legal, statutory, regulatory and contractual requirements	5.31	Yes	Registers are maintained to capture relevant Information Security & Privacy Information related statutory, regulatory, and contractual obligations. Cryptographic Controls are in compliance with all relevant statutory and regulatory and other legal obligation requirements.
Intellectual property rights	5.32	Yes	Appropriate procedures are implemented to ensure compliance with statutory, regulatory, and other legal obligation requirements on the user of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
Protection of records	5.33	Yes	Policies are in place to ensure records are protected from loss, destruction and falsification, in accordance with statutory and regulatory and other legal obligation and business requirements.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Privacy and protection of PII	5.34	Yes	Our Privacy and Personal Data Protection Policy our Data Compliance and Ethics Policy, and our Global Data Subject Rights Policy and procedures, standards, and training support relevant statutory and regulatory and (if applicable) other legal requirements.
Independent review of information security	5.35	Yes	Audits and reviews may be conducted internally by persons independent of the function of management being audited and/or 3rd parties to ensure impartiality of the audit / review processes.
Conformance with policies, rules and standards for information security	5.36	Yes	Leaders are responsible for ensuring compliance within their areas of responsibility. Reports of non-compliance will result in corrective action being required and may identify opportunities for improvement. These are also reviewed and reported at Management Review Meetings. Information technology systems are checked for compliance with security implementation standards.
Documented operating procedures	5.37	Yes	Policies, standards, procedures, training materials and other instructions / information is provided to those that need them to effectively fulfil the Information Security & Privacy Information aspects of their roles.
6 People Controls			
Screening	6.1	Yes	Background verification checks in line with our policies and procedures are carried out for all candidates accepted for employment. Policies take account of relevant regional laws and regulations; are proportional to the business requirements, the classification of information accessed and the perceived risks to the business.
Terms and definitions of employment	6.2	Yes	The contractual obligations for employees and directly employed contractors engaged by Dun & Bradstreet are set out in the Terms & Conditions of Employment which all employees, and directly employed contractors, are required to sign before commencing employment. These terms and conditions also set out the continuing responsibilities for Information Security & Privacy Information after employment ends. We have contractual agreements with third party suppliers whose employees work at Dun & Bradstreet premises, they are often referred to as contractors or contingent workers. Our supplier agreements with these third parties require their employees to comply with our Information Security & Privacy Information policies and procedures.
Information security awareness, education and training	6.3	Yes	A program of mandatory, annual Information Security & Privacy Information Awareness, Education & Training, (including Cyber Security, Privacy and Code of Conduct courses) for all new hires and existing employees. Additional education and awareness is provided on an ongoing basis. Where there are role specific Information Security & Privacy Information requirements, training needs are assessed, and appropriate training arranged.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Disciplinary process	6.4	Yes	We have clear Disciplinary Procedures to handle circumstances where an employee who has committed an Information Security &/or Privacy Information breach.
Responsibilities after termination or change of employment	6.5	Yes	Processes exist to ensure employees are reminded of their obligations regarding Information Security & Privacy Information and the consequences of not meeting those obligations when they leave Dun & Bradstreet. When employees change roles, the responsibility rests with the line manager to advise the employee of any role specific obligations.
Confidentiality or non-disclosure agreements	6.6	Yes	Confidentiality and non-disclosure agreements are established and used where appropriate to protect information.
Remote working	6.7	Yes	Teleworking is common practice in our working environment. Our policies and training take into account the risks and associated controls required.
Information security event reporting	6.8	Yes	We have procedures in place to ensure actual Information Security & Privacy Information events and weaknesses are reported and recorded. These procedures are supported with training courses and policy.
7 Physical Controls			
Physical security perimeters	7.1	Yes	Physical perimeter security, entry controls and the security of confidential spaces is defined by and managed in accordance with our Physical Security Policy. Additional documented information supports the execution of the policy. Security measures, including monitoring, are applied where required or appropriate, in line with the size, scale, and risk identified at individual premises. All deliveries in our offices are made via our reception / mail room teams. Larger equipment deliveries are overseen by our facilities team.
Physical entry	7.2	Yes	
Securing offices, rooms and facilities	7.3	Yes	
Physical security monitoring	7.4	Yes	
Protecting against physical and environmental threats	7.5	Yes	Protection of our facilities, in line with health and safety legislation requirements, is in place. Additional fire, heat and flood protection is active in sensitive secure areas housing essential equipment. Additional security measures are also in place at all our sites to help prevent malicious access.
Working in secure areas	7.6	Yes	We have policies and procedures to ensure that access to secure areas is restricted on a specific needs basis and that special working procedures are in place and rigorously enforced.
Clear desk and clear screen	7.7	Yes	Policy, standards, and training are in place to ensure that users clear their desk of restricted information when unattended and log off or lock devices whenever equipment is left unattended so that passwords or PINs are required to reactivate sessions.
Equipment siting and protection	7.8	Yes	Equipment is sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Security of assets off-premises	7.9	Yes	Security is applied to assets and equipment off-site, taking into account the different risks that arise outside the Dun & Bradstreet premises.
Storage media	7.10	Yes	The use, management, destruction, and physical transportation of removable media is controlled by our policies, standards, and procedures. Equipment, information, and software is not to be taken off-site without prior authorization unless set out in policy.
Supporting utilities	7.11	Yes	Equipment is protected from power failures and other disruptions caused by failures in supporting utilities by ensuring suitable planning and architecture of infrastructure utilities.
Cabling security	7.12	Yes	Power and telecommunication cabling carrying data or supporting information services is protected from interruptions or damaged.
Equipment maintenance	7.13	Yes	Equipment is correctly maintained to ensure its continued availability and integrity.
Secure disposal or re-use of equipment	7.14	Yes	Policy, process, and procedures exist that ensure that all equipment reuse is managed, and disposal is undertaken securely.
8 Technological Controls			
User endpoint devices	8.1	Yes	The requirements for both company-provided devices and employee-owned devices are set out in our policies. Policy, standards, and training are in place to ensure that users log off or lock devices whenever equipment is left unattended so that passwords, PINs or bio-metric IDs are required to reactivate sessions and that sessions should be terminated when no longer in use.
Privileged access rights	8.2	Yes	Allocation and use of privileges are restricted and controlled in line with our global policy.
Information access restriction	8.3	Yes	Access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.
Access to source code	8.4	Yes	Access to program source code is restricted.
Secure authentication	8.5	Yes	Access to operating systems is controlled by a secure log-on policy.
Capacity management	8.6	Yes	Use of resources is monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
Protection against malware	8.7	Yes	Where technically feasible, all Dun & Bradstreet servers and workstations are required to have active anti-malware software that is configured in compliance with Dun & Bradstreet corporate standards. Any server or workstation without active configured anti-malware software may be blocked from network services until brought into compliance.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Management of technical vulnerabilities	8.8	Yes	Technical vulnerabilities are identified and managed in line with our policies and processes. Information technology systems are checked for compliance with security implementation standards.
Configuration management	8.9	Yes	The configuration of hardware, software, services and networks is documented, monitored and reviewed to ensure their correct function and that they are not altered without appropriate authorization.
Information deletion	8.10	Yes	Information stored on our systems, devices or other media is deleted when no longer required in line with our Retention Policy complying with local legislation and any contractual obligations.
Data masking	8.11	Yes	Data masking is used in accordance with our policies to limit the exposure of sensitive data including PII, and to comply with legislation and contractual obligations.
Data leakage prevention	8.12	Yes	Detection and prevention measures are in place to prevent data leakage.
Information backup	8.13	Yes	Back-up copies of information and software are taken and tested regularly in accordance with our back-up policy.
Redundancy of information processing facilities	8.14	Yes	A managed process has been developed and maintained for establishing, documenting, implementing and maintaining processes, procedures and controls to ensure the required level of continuity for Information Security & Privacy Information during an adverse, unplanned or emergency situation.
Logging	8.15	Yes	Audit logs recording user activities, exceptions, and Information Security & Privacy Information incidents, are produced and kept for an agreed time period to assist future investigations and access control monitoring. Logging facilities and log information is protected against tampering, unauthorized access, and destruction. System Administrator / Operator activities are logged, protected from amendment by the same System / Operator Administrator and regularly reviewed.
Monitoring activities	8.16	Yes	Networks, systems, and applications are monitored for anomalous behaviour to enable appropriate action to be taken.
Clock synchronization	8.17	Yes	The clocks of all relevant information processing systems are synchronized with an agreed single accurate time source.
Use of privileged utility programs	8.18	Yes	The use of utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.
Installation of software on operational systems	8.19	Yes	We have policies and procedures in place to ensure the installation of software on production systems is appropriately controlled. Only Dun & Bradstreet approved, licensed, and functionally required, software is installed on end user devices

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Networks security	8.20	Yes	Dun & Bradstreet maintain appropriate controls and procedures to ensure the consistent and secure operations of the network and related components.
Security of network services	8.21	Yes	Dun & Bradstreet ensure security is considered and addressed in all network service agreements.
Segregation of networks	8.22	Yes	Networks are segregated as much as practical to prevent access overlap and to minimise impact of any incident to a network.
Web filtering	8.23	Yes	Access to external websites is managed to protect systems and prevent access to unauthorized websites.
Use of cryptography	8.24	Yes	Policies, standards, and procedures on the use of cryptography controls for the protection of information and for the life cycle of cryptographic keys has been developed and implemented.
Secure development lifecycle	8.25	Yes	Development of software within the organisation is set out in our policy for secure application development. Third Parties are required to meet our standards as set out in our Third-Party Management Policy.
Application security requirements	8.26	Yes	Information involved in application service interactions is protected to ensure that its confidentiality, availability, and integrity is, by design and overall architecture, protected. All systems and supporting infrastructure that pass information over public networks are designed, developed, and operated in a manner that appropriately protects the interests of Dun & Bradstreet and its customers.
Secure system architecture and engineering principles	8.27	Yes	Software security standards are in place to ensure that systems are designed, developed, implemented, maintained, and documented consistently in accordance with security and privacy requirements.
Secure coding	8.28	Yes	Secure coding principles are applied to software development.
Security testing in development and acceptance	8.29	Yes	Systems security requirements and functionality are integrated into software test plans. Software change control, test procedures, and system acceptance procedures are followed when new; or amended hardware, software, and relevant procedures are introduced to the production environment.
Outsourced development	8.30	Yes	Where outsourced development activity is undertaken it is compliant with our global policies; leaders provide suitable and adequate supervision and monitoring of all outsourced development. There is currently no outsourced development in Norway, Sweden or India (DBIS).
Separation of development, test and production environments	8.31	Yes	Development, test, and operational environments are separated by controlled access to reduce the risks of unauthorized access or changes to the operational system. Secure development environments for system development and integration cover the entire system development lifecycle in line with our policy for secure application development.

Control	ISO 27001:2022 Annex A ref.	Control in place	Justification / Remarks
Change management	8.21	Yes	Policies and processes are documented and implemented to ensure that changes likely to impact Information Security & Privacy Information are controlled. When operating platforms are changed, business critical applications are reviewed and tested to ensure no adverse reactions to operations or security. Changes to software packages are discouraged, limited to necessary changes and effective software change control.
Test information	8.33	Yes	Data used for testing systems are stored and processed in a manner that ensures appropriate security controls and compliance with all applicable privacy requirements and where production environment sensitive data is used in a test environment it shall be redacted or otherwise obfuscated.
Protection of information systems during audit testing	8.34	Yes	Audit of operational systems are carefully planned and agreed in advance to minimize disruption to business processes in line with documented policy and procedure.

PIMS control objectives and controls as a PII Controller:

Control	Annex A	Control in place	Justification / Remarks
7.2 Conditions for collection and processing **Objective:** To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.			
Identify and document purpose	7.2.1	Yes	The specific purposes for processing PII are identified and documented in records of processing and/or impact assessments. Purposes are summarized in our privacy and transparency statements.
Identify lawful basis	7.2.2	Yes	The lawful basis for processing PII is identified and documented in records of processing and/or impact assessments.
Determine when and how consent is to be obtained	7.2.3	Yes	We utilize our records of processing and/or impact assessments to document and demonstrate if, when, and how consent is an appropriate lawful basis and when and how it is obtained from PII principals.
Obtain and record consent	7.2.4	Yes	Consent is obtained and recorded where it is required.
Privacy impact assessment	7.2.5	Yes	Where considered appropriate, based on our inherent risk evaluations, Privacy and other forms of Impact Assessment are conducted where there are plans for new processing of PII or changes to existing PII processing.
Contracts with PII Processors	7.2.6	Yes	Written contracts are required with all engaged PII processors and address the appropriate ISO 27701 Annex B controls.
Joint PII controller	7.2.7	Yes	Respective roles and responsibilities are determined with joint PII controllers (applies to certain Dun & Bradstreet entities only).
Records related to processing PII	7.2.8	Yes	Records of processing are created for new data processing activities, and obligations for processing PII are determined and necessary records maintained that describe the processing activities performed and associated risks.
7.3 Obligations to PII principals **Objective:** To ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.			
Determining and fulfilling obligations to PII principals	7.3.1	Yes	Legal, regulatory, and business obligations to PII principals relating to processing of their PII, and the means to meet those obligations, are documented in our privacy notices, policies, and transparency statements.
Determining information for PII principals	7.3.2	Yes	Information that is to be provided to PII principals (and when) is documented in our privacy notices, policies, and transparency statements, and where applicable, in response to data subject access requests.

Control	Annex A	Control in place	Justification / Remarks
Providing information to PII principals	7.3.3	Yes	Information identifying the controller and describing the processing of PII is clearly set out and easily accessible for PII principals in our privacy notices, policies, and transparency statements.
Providing mechanism to modify or withdraw consent	7.3.4	Yes	There are mechanisms for PII principals to modify or withdraw their consent.
Providing mechanism to object to PII processing	7.3.5	Yes	There are mechanisms for PII principals to object to processing of their PII.
Access, correction and/or erasure	7.3.6	Yes	Policies, standards, and processes are in place for PII principals to access, correct, and / or erase their PII.
PII controllers' obligations to inform third parties	7.3.7	Yes	Processes are in place to inform third parties with whom PII has been shared in connection with our products and services should there be any modification, withdrawal or objections relating to shared PII.
Providing copy of PII processed	7.3.8	Yes	Policies, standards, and processes are in place to provide copy of processed PII when requested by PII principals.
Handling requests	7.3.9	Yes	Policies and procedures are in place to handle legitimate requests from PII principals.
Automated decision making	7.3.10	Yes	Obligations to PII principals regarding automated decision making have been addressed.
7.4 Privacy by design and privacy by default **Objective:** To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.			
Limit collection	7.4.1	Yes	Consistent with our policies and processes, collection of PII is limited to the minimum that is relevant, proportional, and necessary for the identified purpose.
Limit processing	7.4.2	Yes	Consistent with our policies and processes, processing of PII is limited to that which is adequate, relevant, and necessary for the identified purpose.
Accuracy and quality	7.4.3	Yes	Documented policies and processes are in place to ensure the accuracy and quality of PII throughout the life-cycle of the PII.
PII minimization objectives	7.4.4	Yes	Data minimization objectives are documented together with processes to meet these objectives.
PII de-identification and deletion at the end of processing	7.4.5	Yes	Consistent with our policies and processes, when no further processing of PII is anticipated it is deleted or de-identified so that PII principals cannot be re-identified.
Temporary files	7.4.6	Yes	Processes are in place, together with periodic checks, to ensure that any temporary files created as a result of PII processing are erased or destroyed.
Retention	7.4.7	Yes	Consistent with our policies and processes, PII is not retained for longer than is necessary for PII processing.

Control	Annex A	Control in place	Justification / Remarks
Disposal	7.4.8	Yes	Documented processes are in place for PII disposal consistent with our practices for disposal of data classified as higher sensitivity.
PII transmission controls	7.4.9	Yes	Appropriate controls are in place to ensure the secure transmission of PII to an intended recipient consistent with our practices for data transmission of data with higher sensitivity.
7.5 PII sharing, transfer and disclosure **Objective:** To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.			
Identify basis for PII transfer between jurisdictions	7.5.1	Yes	The relevant basis for the transfer of data between jurisdictions is documented in our records of processing and impact assessments.
Countries and international organizations to which PII can be transferred	7.5.2	Yes	Documentation is in place consistent with our transfer impact assessments that specifies the countries and international organizations to which PII can be transferred.
Records of transfer of PII	7.5.3	Yes	Records of PII transfers to or from third parties are maintained.
Records of PII disclosure to third parties	7.5.4	Yes	Records of PII disclosures to third parties are maintained.

dun & bradstreet

PIMS control objectives and controls as a PII Processor:

Control Objective / Control	Annex B	Control in place	Justification / Remarks
8.2 Conditions for collection and processing **Objective:** To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.			
Customer agreement	8.2.1	Yes	Contracts to process PII take account and recognise the provision of assistance to meet the customer's obligations.
Organization's purposes	8.2.2	Yes	PII is only processed for the purposes documented in agreements with the customer.
Marketing and advertising use	8.2.3	Yes	Marketing and advertising use of PII processed under a customer agreement is only included where express consent from PII principals has been fairly obtained.
Infringing instruction	8.2.4	Yes	The customer will be informed if a processing instruction infringes applicable legislation / regulation.
Customer obligations	8.2.5	Yes	The customer will be provided with appropriate information to enable them to demonstrate compliance with their obligations.
Records related to processing PII	8.2.6	Yes	Demonstration of compliance with our contractual obligations for processing PII on behalf of a customer are documented in our records of processing and impact assessments.
8.3 Obligations to PII principals **Objective:** To ensure that PII principals are provided with the appropriate information about the processing of their PII, and to meet any other applicable obligations to PII principals related to the processing of their PII.			
Obligations to PII principals	8.3.1	Yes	The customer will be provided with the means to comply with its obligations related to PII principals.
8.4 Privacy by design and privacy by default **Objective:** To ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.			
Temporary files	8.4.1	Yes	Procedures are in place, together with periodic checks, to ensure that any temporary files created as a result of PII processing are erased or destroyed.
Return, transfer or disposal of PII	8.4.2	Yes	The policy and standards concerning the secure return, transfer and/or disposal of PII is available to the customer.
PII transmission controls	8.4.3	Yes	Appropriate controls are in place to ensure the secure transmission of PII to an intended recipient consistent with our practices for data transmission of data with higher sensitivity.
8.5 PII sharing, transfer and disclosure **Objective:** To determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.			
Basis for PII transfer between jurisdictions	8.5.1	Yes	The customer is informed in a timely manner of the relevant basis for the transfer of data between jurisdictions or intended changes in this regard, so that the customer has the ability to object or terminate the contract.

Control Objective / Control	Annex B	Control in place	Justification / Remarks
Countries and international organizations to which PII can be transferred	8.5.2	Yes	Documentation is in place consistent with our transfer impact assessments that specifies the countries and international organizations to which PII can be transferred.
Records of PII disclosure to third parties	8.5.3	Yes	Records of PII transfers to or from third parties are maintained.
Notification of PII disclosure requests	8.5.4	Yes	Notification is provided to the customer of any legally binding requests for disclosure of PII.
Legally binding PII disclosures	8.5.5	Yes	Requests for any PII disclosures that are not legally binding are rejected, accept any that are contractually agreed requests that are authorised by the corresponding customer and consult the customer on any other PII disclosure requests.
Disclosure of subcontractors used to process PII	8.5.6	Yes	Before using any subcontractors to process PII, disclosure will be made to the customer.
Engagement of a subcontractor to process PII	8.5.7	Yes	Subcontractors are only engaged to process PII according to the customer contract.
Change of subcontractor to process PII	8.5.8	Yes	The customer is informed of any changes concerning the addition or replacements of subcontractors to process PII prior to the new subcontractor processing PII.