Cintra HR & Payroll Services

1.	**Security of Storage**
1.1	Measures for the protection of data during storage
	All data is encrypted at rest, and access is strictly limited, either role-based or those with a specific business need. All access requests are logged within the IT Service Desk and require prior approval before being actioned. Regular access reviews are carried out to ensure all access remains appropriate.
1.2	Measures for ensuring physical security of locations at which personal data are processed
	Cintra HR & Payroll Services' office is protected by key card access, of which access is restricted solely to employees. All areas of the building containing sensitive data (storage or processing) are restricted, with access restricted on role or those who explicitly require it for a specific business need. The data centres in which we hold our cloud-based data are Tier 3 and have been certified to both Cyber Essentials and ISO27001 along with a host of other applicable accreditations. The data centres have multiple physical security controls in place, including state-of-the-art CCTV and access controls.
1.3	Measures for ensuring limited data retention
	Data is automatically deleted in line with PSSG's Data Retention policy.
1.4	Measures for ensuring data minimisation
	PSSG has a GDPR team that conduct DPIAs for projects across the entire group as and when required. As part of the DPIA, each project is reviewed to consider evidence as to how it can be ensured that no more data is collected than is necessary for the business need(s). This is then assessed, and the applicable risks considered and recorded.
2.	**Security of Transmission**
2.1	Measures for the protection of data during transmission
	Data transmission is only transmitted via TLS 1.2, and if supported TLS 1.3. All data transmissions are encrypted at the point of transmission.

3.	Security of Processing
3.1	Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
	PSSG has a dedicated IT Team who are responsible for deploying and managing our security tools, in addition to responding to, and reporting on, incidents. The tools in use include, but are not limited to: • Firewalls at all internet borders. • IPS (Intrusion Prevention System) at all internet borders. • WAF (Web Application Firewall) protecting all web applications. • Identity and Access management platform providing identity verification and MFA (Multi-Factor Authentication). • Anti-virus with both signature based and behavioural based detection. • Cloud hosted data centres and failover sites with a minimal switchover time
3.2	Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
	Availability monitoring tools are deployed to all infrastructure with both pre-emptive and reactive alerting configured. Alerts are sent to PSSG's IT Team to investigate and respond to.
3.3	Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
	Cintra HR & Payroll Services is ISO27001:2013 certified, with only one documented exclusion in scope (14.2.7). This is audited on an annual basis to ensure ongoing adherence and compliance to the standard. Throughout the year, PSSG's Compliance department conduct internal audits across all business functions to both ensure compliance and to identify methods of improving information security controls.
3.4	Measures for certification/assurance of processes and products
	PSSG has a dedicated Compliance team who manage all aspects of certification/assurance, including ISO9001:2015 & ISO27001:2013, along with other industry specific certifications. All certifications are externally audited and validated, which provides assurance of our processes.
3.5	Measures for ensuring events logging
	All security log generating equipment is configured to retain logs and report on malicious activity.

4.	Organisational security measures
4.1	Measures for allowing data portability and ensuring erasure
	Cintra HR & Payroll Services has an established data deletion process implemented, and this includes data portability. When a data deletion request is made, a request begins a specific chain of events to remove all data from our systems. At all stages of the process, an audit trail is maintained to validate that the data has been removed and by whom.
4.2	Measures for user identification and authorisation
	All users are provided with unique credentials for all systems, and as per our information security policies, it is prohibited to share those credentials under any circumstance. All access is provided to users under the principle of least privilege and only when it is necessary for the purposes of their role. PSSG's Compliance team undertakes monthly access control reviews, covering all departments, to ensure that employee access to each business system and repository remains accurate.
4.3	Measures for internal IT and IT security governance and management
	Cintra HR & Payroll Services is ISO 27001 certified and has both an IT & Compliance team that work together to oversee all security governance related matters. We undertake regular (monthly) internal audits across our processes, policies, and people to validate adherence with the ISO 27001 standard and applicable legislation.
4.4	Measures for ensuring data quality
	Cintra HR & Payroll Services has a Data Protection policy, which references the principle of maintaining data in an accurate format at all times. All employees are provided with appropriate GDPR awareness training that includes recording and maintaining data accurately.
4.5	Measures for ensuring accountability
	As required within ISO27001, the senior management of Cintra HR & Payroll Services are actively engaged in data protection and information security matters and provide input into the security strategy. There is clear communication, business-wide, to all employees to provide awareness of data protection and information security. Both data protection and information security obligations are included within employee communication and agreements, and results from any incident investigation is recorded within relevant personnel files.

5.	Technical security minimum requirements
5.1	Measures of pseudonymisation and encryption of personal data
	All data is encrypted with AES 256 at rest and TLS 1.2 for data in transit.
5.2	Measures for ensuring system configuration, including default configuration
	Configuration of end user devices, servers and network infrastructure is carried out in line with best practice guidelines. All new builds are subject to testing, including vulnerability management, and all standard builds follow manufacturer guidelines and processes.

Version Number	Details	Approver(s)	Date of review	Date of next review
1.0	Inception of list of PSSG (Cintra) sub-processors	Stephen Pearson / Matthew Hart	22/11/2022	01/05/2023
1.0	Annual review	Matthew Hart	01/05/2023	01/05/2024