Talent in Innovation.
Innovation in Talent.

Security & Compliance - GDPR

SHL exists to help our clients win by providing deep people insights to inform talent decisions. As the global leader in assessment science, we help organizations and their leaders address the most pressing talent priorities by providing an unparalleled view of their workforce. Our unrivalled assessment service, benchmark data, extensive and analytic technology enable companies to influence genuine organizational change and drive tangible business outcomes from having the right people in the right roles at the right time.

Data Protection

In light of recent changes to data protection laws in the European Union, namely the introduction of the General Data Protection Regulation (GDPR) on 25th May 2018, SHL undertook multiple actions in furtherance of our compliance measures and as part of our on-going commitment to providing our clients' market leading security and data management.

1. Appointment of a Data Protection Officer (DPO)

SHL recognises itself as a data processor. Our core activities consist of the processing of personal data on behalf of our clients, the data controllers, which requires systematic, large-scale monitoring. Our processing may also include the processing of special categories of personal data on behalf of our data controller where stipulated.

SHL's Global Data Protection Officer (DPO) was designated on the basis of professional qualities including expert knowledge and qualification in data protection law and practices. If you require further information regarding the DPO please email DPO@SHL.com

2. Policies & Notices

SHL periodically conducts systematic updates of its external and internal facing privacy policies and notices. We have established a GDPR resources section on our SHL.com website. The page includes a series of resources addressing SHL's approach and notices as part of our data protection compliance: the SHL GDPR Whitepaper, On-Demand Webinar, Data Protection Notices for Candidate Support and Online Training Services, and a Frequently Asked Questions page. Clients are able to register to be notified automatically when any of these documents are updated.

In order to properly inform data subjects of the uses of their personal data and the lawful grounds which apply, each SHL platform and point of capture of personal data (as controller and processor) receive Data Protection Notices, which are periodically updated as required.

Policies are updated and/or introduced for the improvement of lawfulness, transparency, limitation, minimisation, accuracy, storage and security of personal data where necessary for the GDPR and other country specific legislation or interpretations. Updates include, but are not limited to, the Data Protection Policy, Information Security Policy, Data Retention Policy, End-User and System Use Policy, and Incident Response Plan.

3. Monitoring & Management

The SHL Global DPO heads a cross-department SHL Data Protection Working Party where relevant individuals meet with the DPO on a regular basis. In addition to an Information Security Officer, SHL also employs a Data Governance Specialist to support and monitor data protection requirements across

the organisation. Additionally, key employees across SHL Legal and IT departments receive regular education and have data protection qualifications as part of the overall compliance program.

SHL conducts multiple Privacy Impact Assessments and Data Protection Impact Assessments (DPIAs) each year and employs outside technical and legal consultancy prior to the enactment of any proposed changes to the processing activities of personal data. The DPIAs form and inform internal data governance framework updates outlining regularly scheduled analysis and updates of data protection practices. Where the need for a DPIA is identified an SHL DPIA template is used, developed from the guidelines supplied by Article 29 Working Party/European Data Protection Board.

SHL manages a Record of Processing Activities (RoPA) for the appropriate management and awareness of personal data uses throughout the organisation, which maintains a record of how data processing changes as the organisation or internal business activities change. This is used to measure and maintain compliance and to understand how the use cases change as each business function develops.

SHL maintains the technical and organisational monitoring of systems, processes and third-parties with a relevant and relative schedule of analysis taking into account the nature, scope and context of the processing activities of the personal data. These include but are not limited to, data loss prevention, email monitoring and investigative functionality, CRM, Financial and marketing systems.

SHL has maintains a Privacy Information Management System (PIMS) for the management of all data protection matters within SHL.

4. Processes & Procedures

Where possible, procedural documents for uses of personal data within individual tasks (e.g. recruitment), have been developed to assist individuals who take a role within an activity, but would not be recognised as data processing activity owner so they are able to understand their data protection responsibility during such tasks.

Data subject rights, breach logging & reporting, employee training and data retention periods have one or more policy aligned to each area and undergo scheduled and/or ad hoc review and enhancement for ongoing improvement to data protection practices.

SHL conducts ongoing processes of technical and physical discovery and destruction of personal data where personal data is: a) no longer required for use; b) no longer required for further legal basis for retention or storage; c) duplicated; d) over captured, where purposes have changed and the data is no longer required on the basis it was first captured. Retention and destruction procedural guidelines are in place for this and also continues to go under periodic review and evaluation.

5. Security

We prioritise data security: We understand and have always taken our security obligations seriously, long before the GDPR. Our commitment to security is demonstrated by our on-going certification programs that have been in place for many years. In particular, we have developed and implemented an ISO 27001 certified Information Security Management System for over 10 years running. Additionally, we have obtained ISO 22301 certification for our Business Continuity Practices and we have ISO 20000 certifications for our ability to professionally maintain, support and manage our IT services using best practices. Further information can be found here.

SHL maintains annual compliance training for all employees and relevant contractors. This training includes data protection practices and cyber security, as well as specialised modules for IT and development staff on data handling further demonstrating the commitment to data protection.

6. Data Deletion

SHL acts as the data processor and only deletes data on the request of the data controller. SHL has a defined data deletion process and has an SLA of 30 days from once the deletion is approved by the client for the deletion to be completed.

7. Complying with International Transfer Rules

In accordance with our current practice we will continue to ensure we do not transfer data outside of the EEA without an appropriate data transfer structure in place. Currently, we have EU Standard Contractual Clauses ("Model Clauses") in effect for transfers outside of the EEA to ensure adequate levels of protection as permitted by the European Commission. We are also updating our policies and procedures in anticipation of the withdrawal of the United Kingdom from the European Union. Regardless of the outcome of Brexit, SHL is still committed to the GDPR and we are currently evaluating possible options with respect to the transfer of data between the UK and the EEA. We rely on self- certification under the EU-US Privacy Shield for transfers to the US. Privacy Shield is a self-certification programme under which organisations can register with and confirm they meet specific privacy requirements.

The Privacy Shield is not expressly referenced in the GDPR, but it is recognised by the European Commission as providing adequate protection. We will continue to monitor any proposed changed to Privacy Shield and Model Clauses following the GDPR and ensure we upgrade our agreements and Privacy Shield certification as required.

8. Examples of Compliance with GDPR Articles

Article 13: The right to be informed

Our assessment platform includes a data protection notice which individuals are presented with prior to taking the assessment. This notice provides information to the individual about the collection and processing that we perform, in accordance with data protection legislation requirements.

As the assessment makes up one part of an overall recruitment process, (and the assessment is generally not your first point of candidate data collection) the Article 13 notice requirements may also need to be satisfied earlier than our assessment platform. You may employ several different methods, such as your careers website, an online application form, or applicant tracking system to receive initial applications, and collect other personal information e.g. CV or résumé information, residential address etc. In each of these systems, a data protection notice that addresses the full recruitment cycle would be required at the point of data collection.

You would need to seek independent legal advice on your compliance obligations under Article 13 GDPR.

Article 15 – 18: The right; of access, to rectification, to erase or to restrict processing

A candidate's request to access, correct, delete or restrict processing of data should be directed to you, as the data controller. We occasionally receive requests directly from candidates to delete their information, or to provide access to their assessment results. We redirect these candidate requests back to as the data controller. We then provide support and information to you as you require to meet your obligation to the candidate.

If we receive such a request directly from you as our client, we already have processes in place to carry out that request, whether that is promptly responding to a data subject access request, or a request for deletion of data.

Clients often ask "how long do you retain data?" As a data processor, we retain data in accordance with our client agreements, meaning we delete data following a request from you, our clients. As part of our GDPR compliance strategy we made improvements within our platform to build in increased automation and efficiencies into our data deletion processes.

Article 20 The right to data portability

The right to data portability only applies:

- to personal data an individual (i.e. a candidate) has provided to our clients as the data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means (it does not apply to paper records).

Given the context of the products and services that we offer, we see this right as being quite closely related to the right to access as noted above and we would direct any such requests back to you as the data controller, and then assist in your decisions to comply.

The information that is collected directly from the individual is limited, and therefore providing this in a "structured, commonly used, machine-readable and interoperable format" can be easily done on a case by case basis. It would be up to you as the data controller to determine the extent of the information that you would make available under this right.

Article 21 - The right to object

A candidate may have a right to object to the processing of their personal data if you, as the data controller, rely on legitimate interests as the legal basis for processing. Candidates are free to choose whether to take an assessment or not. If they object to the processing of data, an individual can simply close out of the assessment and we will not perform any further processing.

If the candidate objects after they have started an assessment, this will become a right to deletion under Article 15

Article 22 Rights in relation to automated decision making and profiling

The GDPR provides a right for individuals not to be subject to any automated decisions unless certain exemptions apply. Our clients often use our services to aid in making decisions as to whether to offer employment or a promotion to an individual. Our best practice guidelines recommend that our assessments should be used as part of an overall evaluation and should not be relied upon as the sole basis for any employment related decisions. For any other use of our assessments we would advise you to seek independent legal advice on your compliance obligations under Article 22 GDPR.

As the data controller, if you inform us you intend to use our assessment as part of an automated decision, we can follow your instructions regarding your approach to any permitted exception, such as sufficient notification to individuals that they may be subject to an automated decision.

9. Continual Improvement

SHL is committed to the continual improvement of its data protection activities. Each improvement is logged so patterns can be understood, and further areas of analysis can be identified.

If you are aware of any areas which can be improved in SHL's data protection activities, please do send an email outlining your suggestion clearly to DPO@SHL.com.

If you have any further questions, please either speak to your account manager or email data.questions@shl.com.

