DATA PROTECTION POLICY (GDPR)

June 2021

POLICY STATEMENT

SYSTRA Ltd is committed to ensuring that all the personal data it processes, including but not limited to that of colleagues, clients, customers, and suppliers is managed appropriately and in compliance with the UK's Data Protection Act 2018 ("UK GDPR"). Where personal data is being transferred into, or out of, the European Union we also seek to comply with the EU's General Data Protection Regulation ("EU GDPR") .

We are committed to implementing a data protection approach to safeguard the personal data we process.

SCOPE

This policy applies to:

- All our colleagues which includes permanent, fixed term and agency colleagues.
- All suppliers (including consultants, contractors and any other individuals who provide services or goods to us).
- Any partner of a JV or Consortium where we act as the Client and they supply goods or services via us to the JV or Consortium.
- Any Client where we process or control Personal Data on their behalf under contract.

This policy applies to all the personal data we process about an individual regardless of the location of where that personal data is stored (e.g. company device or own personal device).

Everyone who undertakes work for us or on behalf of us must read this policy.

RESPONSIBILITIES

SYSTRA Ltd.'s Chief Executive Officer has final authority regarding compliance with this policy, the UK GDPR, the EU GDPR and other relevant regulations.

SYSTRA Ltd.'s Data Protection Officer (as noted below) is responsible for the day to day implementation of this policy, including the updating of, and advising the organisation on data protection matters.

All our colleagues, including permanent, fixed-term and agency colleagues, and anyone who provides goods and services for us, such as suppliers, consultants and contractors have a responsibility for ensuring the personal data they process is done in line with this policy, the UK GDPR, other relevant regulations including, if applicable, the EU GDPR.

Everyone must ensure they:

- only access personal data they need to be able to undertake their work;
- keep personal data secure by taking sensible precautions and follow our internal policies and procedures on information security;
- where applicable follow our Customers policies and procedures when providing them with goods or services;
- use strong passwords to protect electronic information and never share their passwords with other colleagues;
- do not make any unauthorised disclosures of personal data, either within company systems or externally;

- do not misuse personal data;
- regularly review and update personal data to ensure it does not become out of date;
- securely dispose of personal data when it is no longer required and in line with our retention periods; and
- undertake annual data protection refresher training and any other data protection training as directed.

DATA PROTECTION PRINCIPLES

Both the UK GDPR and the EU GDPR set out 7 data protection principles which we must comply with when we process personal data:

1. **Lawfulness, Fairness and Transparency Principle**: processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose Limitation Principle:** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data Minimisation Principle:** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy Principle:** accurate and, where necessary, kept up to date.
5. **Storage Limitation Principle:** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and Confidentiality Principle:** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The **7th** principle is the **Accountability Principle** which requires us to be responsible for, and be able to demonstrate compliance with, the above principles.

Everyone must always comply with these principles when processing personal data.

You must inform the Data Protection Officer immediately if you become aware that any of these principles have been breached or are likely to be breached.

PROCESSING PERSONAL DATA

We process both "personal data" and "special categories of personal data" as defined in the UK GDPR and the EU GDPR. In doing so, we remain mindful of associated conditions imposed on the processing of such special category data.

The categories of individuals we process personal data about include:

- our own colleagues;
- customers (who use one of our services);
- individuals who work within our Customers organisations;

- individuals who are contacted on behalf of our Customers or our Suppliers; and
- individuals who work within our Supplier's organisations.

All personal data is processed in accordance with the UK GDPR and the EU GDPR requirements. When processing special categories of personal data, it is essential to maintain a high degree of confidentiality and ensure increased safeguards are in place to keep this personal data secure.

If you are proposing to collect or process personal data, you must contact the Data Protection Officer before such collection or processing of data begins.

We continually review all our personal data processing (including special category personal data) activities and identify and document the legal basis for the processing of each of these activities. The legal basis we rely on is also recorded in our Records of Processing Activities documentation and in our privacy notice which is available on our website.

The Data Protection Officer monitors and is responsible for approving proposed measures for maintaining and keeping these records up to date.

DATA PROTECTION OFFICER (DPO)

SYSTRA Ltd. has appointed a Data Protection Officer ("DPO"). The DPO is required to undertake certain statutory duties including informing and advising SYSTRA Ltd and its colleagues about their obligations to comply with personal data and privacy laws. They are also required to provide advice to SYSTRA Ltd on data protection impact assessments (DPIA) and to monitor the performance of DPIAs.

The DPO will co-operate with the Information Commissioner's Office (ICO) and act as the first point of contact with the ICO on issues relating to the personal data processing activities of SYSTRA Ltd.

The DPO is also the first point of contact for individuals whose personal data is processed by SYSTRA Ltd. The role of the DPO is required to operate independently and whilst it complements the role of our Compliance Team, it is separate.

PRIVACY NOTICES

To ensure compliance with fairness and transparency requirements of the data protection laws and an individual's right to be informed, we always ensure before personal data is collected directly from individuals that they are provided with a privacy notice which tells them why we are collecting their personal data and what we will do with it.

When personal data is obtained from a third party and not directly from an individual, we will issue the individual with a privacy notice when we first communicate with them or within one month from obtaining their personal data, whichever is first.

Our privacy notices will be presented in a way that is concise, transparent, easily accessible, and written in clear and plain language so that an individual can easily understand what happens to their personal data when we use it.

INDIVIDUALS RIGHTS

Under the UK GDPR and the EU GDPR, individuals have the right:

- to be informed;
- of access to their personal data, commonly known as a Subject Access Request;
- to rectify inaccurate personal data;
- to erase their personal data, commonly known as the right to be forgotten;
- to restrict the processing of their personal data;
- to data portability, i.e. to transfer data from one provider to another;
- to object to the processing; and
- not to be subject to a decision based solely on automated processing.

The DPO must be notified immediately of a Subject Access Request from an individual. The DPO will provide you with advice and guidance on how to comply with the request.

The information will be provided to the individual in writing, including electronically and may, at the request of the individual, be given verbally.

All information will be provided without any undue delay and at the very latest within one month of receiving a valid request. All information will be provided free of charge to the individual.

DATA PROCESSORS

If a data processor is used to undertake the processing of any of our personal data, we will only use processors who can provide sufficient guarantees to implement the appropriate technical and organisational measures to be able to comply with the UK GDPR (and the EU GDPR where applicable) and protect the rights of the individuals.

A written data processor contract in a form approved by the DPO must be in place with a data processor before any processing begins.

DATA SHARING

Data sharing is when personal data is shared between organisations which are controllers. Data sharing can take place in a routine scheduled way, or on a one-off basis. Data can also be shared in an emergency when needed.

Any sharing of personal data with other organisations and third parties will be undertaken legitimately and in line with statutory requirements.

For all routine scheduled data sharing it is important that a Data Sharing Agreement is in place with the organisation(s) who we are sharing the personal data with.

DISCLOSURE OF DATA TO THIRD PARTIES

In certain circumstances, the UK GDPR and the EU GDPR allow personal data to be disclosed to third parties who have requested it without obtaining the consent of the data subject.

When a third party does send such a request to us, the DPO must be immediately notified. The DPO will review the request and decide on whether to release the personal data; and will maintain a log of requests from third parties and document the outcome of the decision-making process.

SECURITY OF PERSONAL DATA

We will implement the most appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the personal data we process.

Everyone must ensure that they process personal data securely and do not disclose it to any unauthorised individual or third party either accidentally, negligently or intentionally.

SYSTRA Ltd is accredited to the UK Government CyberEssentials standard.

TRANSFER OF DATA TO A THIRD COUNTRY

We will only transfer personal data to a country outside of the UK when the transfer rules under GDPR are complied with. Transfers of personal data can be made under the "adequacy decisions", or when appropriate safeguards are in place, or when the transfer is covered by an exception as defined under the UK GDPR or the EU GDPR.

The Chief Executive Officer is responsible for approving transfers of personal data outside of the UK and EU. The DPO must be consulted before any transfers of personal data are made outside of the UK and must approve the safeguards that will be implemented for the transfer.

PERSONAL DATA BREACHES

We are responsible for implementing appropriate measures to safeguard personal data we hold from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access.

We will make every effort to protect the personal data we collect or process and reduce the risk of a data breach however we recognise that we cannot entirely eliminate this risk.

Where a personal data breach occurs, or is suspected, it must be reported immediately to the DPO and our UK Compliance Team.

All personal data breaches will be assessed on a case by case basis to determine, within the first 72 hours of discovery, if they are reportable to the Information Commissioners Office and the individuals affected.

A personal data incident log including all breaches (whether reportable or not) will be maintained by the DPO. This will be reviewed regularly to identify trends or regular instances of the same type of breach.

DATA PROTECTION IMPACT ASSESSMENTS

The UK GDPR and the EU GDPR require us to carry out a Data Protection Impact Assessment (DPIA) before we begin any type of processing that is likely to result in a high risk to individuals.

Everyone needs to be aware of the requirement to undertake DPIAs and when the need for a DPIA is identified, the DPO must be consulted before the DPIA is undertaken.

TRAINING

All colleagues will receive annual data protection awareness training, which is compulsory. All new starters will receive data protection training as part of our induction process.

Colleagues in specialist roles that handle personal data and special categories of personal data will receive specific data protection training relating to the type of personal data they process.

If a colleague considers that they would benefit from refresher training earlier than planned, they should speak to their line manager.

FAILURE TO COMPLY

We take our compliance with data protection and this policy very seriously. Failure to comply puts our business at risk from enforcement action, monetary penalties and reputational damage.

Any breaches of the UK GDPR, the EU GDPR, this policy and any procedures or guidance documents governing the use of personal data will be investigated by the DPO and Compliance Team.

Any colleague who is found to be in breach of the UK GDPR, the EU GDPR or this policy, may be subject to formal proceedings under our disciplinary process and, where necessary, may have their access to personal data withdrawn.

If we fail to comply with the UK GDPR or the EU GDPR and that failure causes significant damage or distress to an individual, the Information Commissioners Office can impose severe monetary penalties.

MONITORING

The DPO will monitor compliance with this policy on an ongoing basis.

POLICY GOVERNANCE

This policy was reviewed and updated in June 2021.

The policy will be reviewed on an annual basis and the Company reserves the right to make changes to the policy as appropriate and in line with legislative changes or amendments to our working practices.

This policy does not form part of any colleague's contract of employment and it may be amended from time to time.

Nick Salt

CEO

SYSTRA LIMITED – UK & IRELAND

June 2021