GDPR COMPLIANCE STATEMENT

Introduction

The EU General Data Protection Regulation ("GDPR") came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The 21st Century brings with it a broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals a stronger, more consistent rights to access and control their personal information.

Our Commitment

Astra Group ('we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles.

Astra Group are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We Comply With GDPR

Astra Group maintains a consistent level of data protection and security across our organisation to ensure GDRP compliance.

Our compliancy includes:

Information Audit - Carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

Policies & Procedures - Data protection policies and procedures fully compliant with the GDPR and any relevant data protection laws, including:

Data Protection – Our policy and procedure document for data protection is fully compliant with the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

Data Retention & Erasure – Our data retention policy and schedule ensures that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

Data Breaches – Our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and all employees are aware of the reporting lines and steps to follow.

International Data Transfers & Third-Party Disclosures – Where the Astra Group stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data.

Our compliancy includes:

Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

Subject Access Request (SAR) – Our SAR procedures accommodate 30-day timeframe for providing the requested information and for making this provision free of charge. Our procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

Legal Basis for Processing - We identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR

Privacy Notice/Policy – Our Privacy Notice(s) ensures that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

Obtaining Consent - Our consent mechanisms for obtaining personal data ensures that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time

Direct Marketing - We have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

Our compliancy includes:

Data Protection Impact Assessments (DPIA) – Where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data we carry out impact assessments in line with the GDPR's Article 35. Our documentation processes record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

Processor Agreements – Where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting etc.), GDPR Compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations are in place. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, and the technical and organisational measures in place.

Special Categories Data - Where we obtain and process any special category information, we do so in complete compliance with the Article 9 GDPR and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) GDPR. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via www.astraasia.com & www.astrafs.com of an individual's right to access any personal information that Astra Group processes about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source

Our compliancy includes:

- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

Astra Group takes the privacy and security of individuals and their personal information very seriously, and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- SSL Certificates
- Single sign-on process
- Azure active director auditing all login's and access through the company database and intranet.
- 2 stage account encryption requiring password and phone number
- System Data loss prevention (DLP) policy
- · Microsoft GDPR dashboard

GDPR Role and Employees

Astra Group have designated Dom Hartland as our Data Protection Officer, and have appointed a data privacy team to ensure full GDRP compliance. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Astra Group understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR, and have involved our employees in our continuous GDPR training and updates on best practices.

If you have any questions regarding GDRP and data protection at our firm, please contact Dominic Hartland.

You may also file complain regarding data protection with

Úřad pro ochranu osobních údajů / The Office for Personal Data Protection1
Pplk. Sochora 27
Prague 7, 170 00 Czech Republic
tel.: +420 234 665 800 E-mail: posta@uoou.cz