Data Protection Policy Statement

What is Data Protection

Data Protection Legislation provides legal rights to living individuals or "natural persons" (called Data Subjects) in respect of the personal information which is collected and processed about them. Personal Data is that data relating to a Data Subject who can be identified from that data (or from that data and other data in our possession). It is therefore essential that Personal Data or "personally identifiable information" is processed in a fair and lawful manner and that we are transparent about how we collect, store, transmit and process data including how it is disposed of when it is no longer needed.

We are committed to:

We are fully committed to compliance with Data Protection Legislation and regards the lawful and fair treatment of personal information as a fundamental obligation. To ensure that personal information remains accurate, used for the right purpose, safe, secure, and lawfully held we are committed to:

- Obtaining and processing personal data fairly, lawfully, in a transparent manner and in a way that is relevant and limited to what is necessary in relation to the purpose in which the data will be processed.
- All data that we control, or process is classified by a data owner and handled in a way appropriate to the classification.
- Maintain data retention schedules for all information assets and information is disposed of in line with these schedules.
- Any personal data will be kept securely in an identifiable format for no longer than is necessary.
- Maintain ISO 27001 Information Security Management Systems certification.

Who is responsible for implementing this Policy

Everyone is responsible for implementing this policy, whether employees contractors or agency workers including those employed in businesses within the ColX Group or shared group activities.

Key Requirements

Awareness

We must ensure all workers within their operations are aware of their data protection responsibilities, paying attention to:

- Completion of all Data Protection Training within required timescales (mandatory and recommended).
- Ensuring that they and the rest of the business know who the Data Privacy Lead ("DPL") is in their business area/division and how to contact them.
- Obtaining data protection subject matter advice on new products, processes, and projects and to complete where necessary a Data Protection Impact Assessment ("**DPIA**") or a Privacy by Design and Default Assessment ("**PbDD**").
- Ensuring Information Asset Registers ("IARs") are completed for all personal data processing (and for keeping them up to date).
- Understanding our contractual obligations with its clients regarding data privacy and protection (including instructions for processing and consents for sub-processing and whether we are acting as a Data Processor or Independent Data Controller).
- Information Security and the need to ensure effective protection against unauthorised access to personal data.
- Ensuring all data incidents/breaches are reported in a timely manner in accordance with Data Breach Reporting Standard. Note that our DPO must report data breaches to the Information Commissioners Office ("ICO") within 72 hours of an incident being identified if it is serious and meets the threshold for reporting to the ICO.
- Where processing of personal data is required to be carried out outside of the UK/EEA appropriate governance and safeguards are followed, including completion of a Transfer Impact Assessment ("TIA") and the use of International Data Transfer Agreements incorporating ICO approved standard contractual clauses ("SCCs").
- Where direct marketing is being planned for us or for clients, ensuring that personal data can only be used where data subjects have expressly provided consent to receive such material.
- Responding to Subject Access Requests (and other rights including, for example, data portability, data deletion etc.) within 30 days of receipt.

Data Protection Registrations

As a Data Controller, we are registered with the Information Commissioners Office (ICO) which is the UK Data Protection Authority. Senior Management must ensure that the data protection registrations are accurate and up to date.

Data Breach Reporting

Where we act as a Data Controller, data breaches that meet the threshold for reporting must be reported to the ICO within 72 hours. It is the responsibility of our DPO to report breaches to the ICO and sometimes to data subjects. The DPO will also be responsible for determining whether the reporting threshold to the ICO has been met in respect of each incident. Data breaches where we act as Data Processor must be reported to the Data Controller (client) in accordance with the operational requirements and our contractual obligations.

Data Protection Impact Assessments

A DPIA will determine the level of privacy risk arising in a project. For guidance on when a DPIA is needed please refer to the DPO. A DPIA will address the nature, scope, context, and purpose of the processing. DPIA's are an essential part of good data governance and will help us understand and document our data processing activities and identify any associated risks and drive our controls and security requirements.

Following our DPIA, we will be able to clearly address any privacy risks and identify the impact, harm, or damage of processing to the individuals. Keep these under review and communicate any changes, issues or problems to our DPO. The ability to produce a DPIA is also critical to our defence should we be subject to a formal investigation by the Data Protection Supervisory Authorities.

Client Relationship

We acknowledge that within the context of its services it can be working as an independent Data Controller or Data Processor, and this will be captured within the contractual arrangements in place with our clients. Where we are considered a Data Controller, we must fulfil our obligations under the Data Protection Legislation in respect of safeguarding an individual's data and reporting any breaches. Where we act as a Data Processor, it is important we only process personal data in accordance with client's instructions. All instructions for processing personal data for a client must be in writing and the appropriate consents obtained for any sub-processing whether this is within the UK, EEA or outside of the UK/EEA (e.g., India, South Africa, USA, etc.). These procedures should typically cover the processing of the personal data, any security requirements, handling complaints, subject access requests and breach reporting.

Employees are responsible for ensuring that all data breaches (whether we are the Data Controller or a Data Processor) are reported and that data breach reporting procedures are followed.

Non-Compliance

- Non-compliance with this Standard may result in disciplinary action.
- If Managers identify that their teams are not operating in a compliant manner with this Standard this should be reported to the DPO.
- If Managers wish to seek a waiver for any aspect of this Standard, they must seek written approval from the DPO.

Approvers

Paula Jacobs
Chief Operating Officer
(Director)

Simon Jacobs
Chief Executive Officer
(Director)