XPERT·STEM

GDPR and Data Protection Policy

Document Number: QMS-WI-COM-003
Revision: March 2026

1. Purpose and Scope

This policy outlines how **XPERTSTEM** ("the Company") ensures the protection of personal data and the safety of vulnerable individuals. It applies to all employees, international consultants, and third-party partners regardless of their location.

- **Universal Protection**: We apply UK GDPR standards to all personal data we process, regardless of the customer's nationality or location.
- **Zero Tolerance:** The Company maintains a zero-tolerance approach to any form of abuse or exploitation of children or vulnerable adults.

2. International Data Transfers & Consultants

As a UK-based controller, any access to personal data by consultants outside the UK is a "restricted transfer".

- **Transfer Safeguards**: Data will only be transferred to countries with UK Adequacy Regulations or where an International Data Transfer Agreement (IDTA) or UK Addendum is in place.
- **Direct Collection**: Consultants collecting data directly from customers must upload it immediately to the Zoho CRM. Local storage on personal devices is strictly prohibited.
- **Risk Assessments**: A Transfer Risk Assessment (TRA) must be completed for every non-adequate country where a consultant operates.

3. Data Protection Principles (Zoho & Beyond)

- **Data Minimisation**: Only the minimum amount of data required for the consultant's specific task should be collected or processed.
- **Security by Design**: All data in the Zoho CRM is encrypted. Consultants must use multi-factor authentication (MFA) to access the system.
- **Retention**: Data is kept only as long as necessary. Once a consultant's contract ends, their access is revoked immediately, and any temporary local files must be securely deleted.

XPERTSTEM adheres to the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

4. Child Safeguarding & Code of Conduct

All staff and consultants interacting with customers (digitally or physically) must adhere to the **Global Safeguarding Code of Conduct**:

- **Reporting Concerns**: Any suspicion of harm to a child must be reported to the **Designated Safeguarding Lead (DSL)** within 24 hours.
- **Digital Interaction**: Consultants must never contact a child or vulnerable person via personal social media or private messaging apps for company business.
- **Safe Recruitment**: All international consultants undergo background checks (where legally available in their jurisdiction) and mandatory safeguarding training before starting.

5. Individual Rights

All customers, regardless of their location, have the following rights under our policy:

- **Right to Access**: Customers can request a copy of the data held about them.
- **Right to Erasure**: Customers can request the deletion of their data from our Zoho system at any time.
- **Transparency**: Privacy notices must be provided at the point of data collection by the consultant.

6. Enforcement and Non-Compliance

Failure to comply with this policy may result in the immediate termination of the consultant's contract and, where applicable, referral to regulatory authorities (such as the ICO) or local law enforcement.