Data Privacy Management Framework

XCD HR Limited

01 November 2017

Contents

Document Control

Document Name	Data Privacy Management Framework XCD HR limited
Version Date	V0.2November 2017
Status	FINAL
Classification	Restricted
Document Author	Chris Mitford-Slade (CMS)
Approved By	Simon Fowler (SRF)
Next Review Date	01 November 2018

Version Control

Version	Date	Comments and Amendments	Updated By
V0.1		Fifth Step proposed draft	
V0.2	15/11/2017	XCD update	CMS

1. Purpose

The purpose of this Data privacy management framework document is to describe the Privacy Management programme of XCD HR and to support GDPR compliance within XCD HR.

This framework serves as a strategic framework to assist XCD HR in building a robust privacy infrastructure supported by an effective on-going review and monitoring process to facilitate compliance with the requirements of GDPR regulation.

2. Objectives

The objective for Privacy Management programme of XCD HR and associated framework is

- to develop and maintain the plans, procedures and processes required to support the mission set out in the Information Security and Data privacy policy of XCD HR.
- to demonstrate XCD HR's commitment to good corporate governance and building trust with its employees and customers through open and transparent security, privacy policies and practices.
- to demonstrate due diligence, and potentially raise the protection of personal data that they hold to a higher level than the bare minimum needed to meet legal requirements.

3. Scope

The scope is defined in terms of the XCD HR organizations, locations, stakeholders, products / services and processes encompassed by the data privacy programme.

3.1 Organizations/Locations in Scope

Privacy framework and this document applies to XCD HR and all its Operational Units (Departments). It applies to all staff, contractors and third party vendor personnel working within those locations.

3.2 Stakeholders

The stakeholders directly involved in implementing or contributing to privacy framework for XCD HR include employees, contractors, suppliers and clients/partners of XCD HR businesses in the scope.

3.3 Key Products, Services and Processes

XCD HR is a global provider of a comprehensive, fully integrated, cloud based HR and Payroll solution that uses the Salesforce platform. The XCD solution is a fully comprehensive HR Information System (HRIS) which manages the entire employee lifecycle from hire to retire. This is a unified solution, built on the Salesforce platform, with all data processing being contained within the system (including Recruitment, on-boarding, UK payroll, talent management, resource planning and salary reviews).

XCD HR offers a solution for small, medium to large businesses across all industries. XCD HR is able to cater to not only Mid Enterprise and Public sector organizations but also any organisation outside of these remits. Privacy framework of XCD HR covers privacy controls built into this solution to meet the requirements of the GDPR regulation.

4. Data Privacy Management Framework

While establishing privacy management framework for XCD HR, it is assumed that:

- The privacy controls and processes required to deliver and support the key products and services are same across all the locations of XCD HR (this includes XCD HR Limited with offices in Bristol, UK and XCD HR Private Limited, with offices in Bangalore and Kolkata, India). XCD HR operates as a single company with all operational functions (Product Management, Development, Support, HR, Finance and Legal) working across both UK and India, hence privacy controls and processes will be the same.
- The resources required establishing privacy management framework and activities are similar in each operational units but may need to be amended depending on local requirements.

4.1 Regulations and Standards

Privacy management programme will comply with the regulations for UK and Europe. Legislative requirements outside of these jurisdictions are the responsibility if the client. The XCD HR solution, and processes, can be adapted if requested by the client.

4.2 Governance Structure

In order to ensure on-going effectiveness, compliance and accountability, GDPR requires an organisation to ensure support from top management and defines set of responsibilities across various roles within the framework. Top management support is key to a successful privacy management programme and essential for privacy respectful culture.

XCD HR Board: provides necessary sponsorship to the establishment of privacy management framework and programme within XCD HR. The Board of Directors are responsible for defining the objectives and approval of the Data Privacy policy and plans, as appropriate. The Board of Directors has appointed a DPO for each company within XCD HR:

- DPO for XCD HR Limited: Chris Mitford-Slade
- DPO for XCD HR Private Limited: Amjad Khan

Data Protection Officer (DPO): is required to report directly to the highest management level of the organisation. DPO's role involves at least the following tasks:

- Inform and advise XCD HR management and its employees, who carry out processing of personal data, of their obligations under the GDPR.
- ongoing assessment and monitoring compliance with privacy programme and GDPR requirements.
- provide advice, when requested, regarding privacy impact assessment and monitor its performance.
- coordinate with stakeholders and Supervisory Authorities.
- act as a point of contact for the Supervisory Authorities on issues relating to processing.
- establish and implement privacy controls;
- Deal with the request received from data subject (reference to various rights assigned to data subject under GDPR regulation)
- Coordinate with operational units for training all staff/contractors on awareness about the GDPR requirement.

CEO (accountable to the Board) is responsible for directing and overseeing privacy management framework and activities across XCD HR. Responsibilities are as follows:

- Monitor and review the privacy management framework and programme and its compliance within XCD HR.
- Monitor and review performance against privacy management objectives and deliverables.
- Monitor and review resources required to deliver privacy management framework.

The Executive Team are responsible for delivering the privacy management programme across their functional area and responsibilities include:

- Implementing data security processes and procedures in accordance with the this framework
- Review and audit of processes and procedures to ensure compliance
- Training and awareness on data privacy and security

5. Data Privacy Management Programme

5.1. Data Inventory and Classification

Understanding and documenting the types of personal data that an organisation collects and where it is held, does affect the type of consent the organisation obtains from individuals and how the data is protected; and it will make it easier to assist individuals in exercising their data access and correction rights.
XCD HR hold large amounts of data across multiple systems; All data is identified, classified and labelled in order to meet GDPR requirement as per XCD HR's Information Classification standard.

5.2. Risk Management methodology

GDPR regulation mandates risk based approach that contemplates potential harm to individual, which means Organisation's controls shall be developed according to the degree of risk associated with the personal data processing activities. In order to establish this risk management framework, XCD HR has designed their risk management framework to address major data security and privacy risks having impact on business and reputation of XCD HR.
Privacy related obligations and risks should be correctly identified and appropriately taken into account in developing business models, related technologies and business practices before new products or services are launched. Risks of data breaches shall be minimized and the effects of any data breaches mitigated.

The fundamentals of every risk assessment process is based on the principles that organization must:

- Identify threats that could do harm and thus indirectly affect organization. Such threats could be from various sources such as intruders, breaches, criminals, and even disgruntled employees.
- Identify and rank the value, sensitivity, and criticality of data by determining the level of risk that data carries if compromised.
- Apply cost-effective actions to mitigate or reduce the risk

XCD HR has adopted the following methodology to establish the risk management framework:

- Identify and understand where, why and how personal data is being processed.
- Perform Risk assessment
    - Identify potential threat
    - Design risk matrix
        - Risks can be classified on 3 risk levels: Low, Medium, High.
        - Common risk impact categories to be considered when assigning risk levels are legal, regulatory, operational, strategic, market, financial, reputational.
    - Determine inherent risk by evaluating threats against risk matrix
    - Identify areas for Data Privacy Impact Assessment (DPIA)
    - Each of the risk considered can become "high risk", depending on the "likelihood and severity" of the risks as determined in a risk assessment process by reference to the nature, scope, context and purpose of processing;
- Data Privacy Impact Assessment (DPIA)
    - Determine specific threats for new technology
    - Analyze high risk areas
- Perform Gap Analysis
    - Identify technical measures

- Identify Organisational measures
- Evaluate effectiveness of measures to mitigate risks
- Determine residual risks – Is it acceptable or not?

- Design risk mitigation action plan
- Identify new or improved technical & Organisational measures to reduce the risk to an acceptable level.
- Design Privacy compliance programme
  - Define policies and procedures
  - Implement new technical measures
- Monitor Privacy compliance
  - Set up alerts and warnings systems
  - Audit / assess measures for effectiveness of the controls
  - Define mechanism to identify new privacy risk areas

5.3. Data Privacy Impact Assessment (DPIA)

Data Privacy impact assessments will be performed on all existing "High Risk" systems with customer data repositories by qualified personnel. Impact assessments will be carried out on critical systems when substantial changes have been undergone.

5.4. Vendor Management Programme

The assessment of the privacy management capability of suppliers and partners forms an element of the data privacy management programme. The purpose is to ensure, as far as possible, that critical suppliers have robust framework to ensure personal data protection within XCD HR.

5.5. Maintenance and Review of Framework

In order to demonstrate that XCD HR has the capacity to comply and has complied with the GDPR regulation, on-going maintenance activities as listed below are considered by DPO:

- Execution of contracts (or agreements) whenever XCD HR need to transfer personal data to other vendors for processing, to ensure that the data is protected in a manner aligned with XCD HR's privacy management framework.
- To ensure that there are systems in place to respond to data access and correction requests from individuals for their personal data, and to respond to complaints from employees and customers about infringement of personal data privacy.
- Review and put in place internal data privacy policies and processes.

- Periodic management review will be carried out to identify change in any requirement to be considered in privacy framework. Feedback from the management will be taken into consideration for improving the privacy management programme.
- As part of the annual review of the privacy framework, review and approval of the following from XCD HR management:

a.	Result of risk Assessments	12 mouths
b.	Result of privacy impact assessment	As needed
c.	Privacy policies and processes	12 months
d.	Privacy framework	12 months

- Additional reviews may be required in the event of any significant organisational changes.

5.6. Training & Awareness

Up-to-date training and education requirement for all relevant team members, tailored to specific needs, is key to an effective privacy management programme.

XCD HR will implement a training programme covering data protection generally and the areas that are specifically relevant to their business model.
XCD HR will implement a policy for determining when training should take place and when refresher training should be carried out and a process for recording when training has been completed.
All relevant team members (i.e. those handling personal data) of an organisation to be aware of, and be ready to act on personal data protection obligations. Those who handle personal data directly may need additional training specifically tailored to their roles.
Training is provided to all stakeholders that include Chief executives, employees and Head of operational units as follows:

- All new starters are introduced to data privacy as a part of their induction process.
- A refresher message on data privacy is issued to all employees at least once every year.
- Suppliers and partners are informed of the company's commitment to data privacy via the Vendor management programme.

5.7. Incident and breach Management

The GDPR introduces new timeframes for notifying Supervisory Authorities and data subjects and requirements regarding the details that are required to be recorded and provided in such circumstances.
XCD HR will:

- put in place, as appropriate, incident/breach response and notification plan to meet 72 hour deadlines in respect of notifications to the Supervisory Authority on behalf of the controller whose data is being processed.
- put in place incident/breach response plan to evaluate situations exposing data subjects to high risk and procedure to enable notifications to be made to data subjects "without undue delay" in such circumstances.
- ensure that processor agreements have provisions allowing controllers to meet the 72 hour deadlines for reporting breaches to the Supervisory Authority.
- ensure that mechanisms are in place to enable it to report data breaches without undue delay to the controller.

6. Change Management

Proposals can be made on how to improve or alter this document. These proposals should be directed to the CEO, who is the owner of this document and as such responsible for proposing an amended policy and requesting sign-off.
This framework shall be reviewed at least annually in order to ensure that it remains relevant and effective.
The Board are responsible for approving this Framework document and any subsequent changes. The Board must approve major changes in advance of them being implemented. CEO may approve minor changes, subject to ratification by the Board.

7. Associated Procedures

Associated procedures are those that implement the policy within the Company. The list of procedures will be reviewed and updated as part of the Policy review.

Procedure Document	Notes
Data classification standard	
Vendor management process	

8. Glossary

BoD: Board of Directors of XCD HR
COO: Chief Operating Officer
CEO : Chief Executive Officer
DPO : Data Protection Officer
DPIA : Data privacy impact assessment

9. Definitions

GDPR: The General Data Protection Regulation coming into force in 2018.

Data subject: The living individual who is the subject of personal data, such as an employee or an individual customer or contact.

Personal data: Information about a living individual held digitally or in a highly organized paper file. There are different categories of Personal data: 'special categories of personal data' is the subset of personal data, which used to be known as 'sensitive personal data'. It includes categories of data, which warrant special treatment, such as health data and ethnicity, and now also biometric data.

Risk: The risks to the rights and freedoms of individuals of "varying likelihood and severity" may result from personal data processing which could lead to "physical, material or non-material damage" (Recital 75)

Privacy management programme: On-going management and governance process supported by top management and appropriately resourced to implement and maintain data privacy management framework.