Module	**PRIVACY & DATA PROTECTION**
Jurisdictions	**UK**
Legal Expert	**CHRISTOPHER HUTCHINGS** Defamation and Privacy Partner https://hamlins.com/people/christopher-hutchings/ https://www.linkedin.com/in/christopher-hutchings-51a7b933/

Module Application

Has your organisation updated its systems to comply with the post-Brexit UK GDPR framework and the EU GDPR (where it applies to an organisation)?

Are relevant staff in your familiar with the current UK (post-Brexit) system for international transfers of personal data?

Do those within your organisation understand their individual obligations and responsibilities when collecting and/or processing personal data under the UK framework?

Module Scope

Following the end of the Brexit transition period on 31 December 2020, the UK modified and amended its data protection framework. This means that every UK-based organisation (or any organisation that processes personal data of UK nationals) must review its operations to assess whether they meet with the UK requirements and also determine if the EU GDPR continues to apply to it (alongside the UK GDPR).

An organisation is therefore required to have in place systems and processes that ensure the collection and/or processing of personal data is in line with the 6 data protection principles. In addition, it must have a resilient network and information system to withstand potential cyber (and non-cyber) attack so as to protect the data and prevent any accidental or unlawful loss or alteration of personal data.

The PRIVACY & DATA PROTECTION module addresses the GDPR framework through a set of 14 core obligations and sub-obligations that an organisation must take into account when building its data protection strategy, including data protection within the workplace.

The core legal and regulatory obligations are based on the following considerations:

- Lawfulness, Fairness and Transparency;
- Decision making;
- Accountability;
- Direction; and
- Control.

An organisation must ensure its staff, contractors and agents (including any processors that are engaged by the controller) are familiar with the legal obligations to which it is subject, as well as their individual legal responsibility. In so doing, an organisation must also take into account any guidance issued by the regulator, the Information Commissioner's Office (ICO) and any sector or industry-specific guidance.

The aim of the module is to equip the subscriber with a practical and clear understanding of their obligations under the UK (and EU, where applicable) framework and to provide an answer to the following questions:

- What are our legal obligations?
- What is the source of those legal obligations?
- How may we ensure that we are complying with our legal obligations?
- What are the consequences of non-compliance?

The PRIVACY & DATA PROTECTION module recognises the most serious breach for an organisation is the accidental or unlawful loss, destruction or alteration of personal data, however it is caused. The ICO expects an organisation to have in place robust breach detection, investigation and internal reporting procedures to prevent a cyber (and/or non-cyber) incident, whether deliberate or otherwise. The penalty for an infringement may result in penalties of up to the higher of £17,500,000 or 4% of the annual worldwide turnover of the group to which the organisation belongs. In addition, the ICO may, in appropriate cases, impose a number of other measures, which include Information Notices, Assessment Notices and Enforcement Notices.

The consequences vary considerably, depending on the nature and extent of the breach or failure. It is, therefore, vital that all staff are fully trained and equipped to discharge their duties, which includes having an understanding of both individual and organisational legal risk and exposure. Indeed, the ICO has specifically emphasised the need for an organisation to provide on-going staff training that needs to be in-depth and tailored to the context of the organisation's processing activities (as well as industry-specific factors); for example, relevant staff at a financial institution are required to conduct customer due diligence, but the level of personal information required will vary depending on whether it is simplified or enhanced due diligence.

At LexisNexis we appreciate the importance of helping non-legal staff understand such obligations. The PRIVACY & DATA PROTECTION module provides this in an easy-to-understand format that can be readily referred to and used by all staff and that incorporates the legal obligations and the consequences of breach, as well as the guidance and recommendations issued by the UK ICO to provide an organisation with practical assistance in the implementation and maintenance of best practice processes throughout its operations. The module also covers any exemptions, the rights of a data subject and the processing of personal data (including criminal offence data) in the workplace by an employer.

The module is divided into 14 core obligations and sub-obligations to help an organisation understand the full extent of its obligations, necessary actions and legal consequences in the event of a breach. The module examines:

- Applicability of Data Protection Laws
- Organisational Governance
- Openness and Transparency
- Collecting Personal and Sensitive Information

- Anonymity and Pseudonymity
- Using and Disclosing Personal Information
- Cross-border Transfers of Personal Information
- Ensuring the Quality of Personal Information
- Ensuring the Security of Personal Information
- Enabling Individuals' Rights
- Managing Complaints and Investigations
- Integrity and Confidentiality
- Surveillance
- Workplace Data Protection

The focus of the PRIVACY & DATA PROTECTION module is the obligations and consequences (including offences) created by the UK GDPR and DPA 2018 (as amended). It does not address the full range of UK privacy law, such as the tort of misuse of private information.

Post-Brexit, the PRIVACY & DATA PROTECTION module has been updated to reflect UK law (UK GDPR and the Data Protection Act 2018, as amended) and does not cover EU regulations or directives (unless applicable). The module sets out the rights of individuals, but does not contain detailed analysis of actions by individuals who have suffered damages or losses due to breaches of its data protection obligations by UK organisations, nor does it cover the process that an entity or an individual would follow to report or seek compensation for the breach and any loss.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.