Memo to Directors: FAMATEL UK LTD
General Data Protection Regulation (GDPR) 24/05/2018

This is the type of memo that can be given to the directors of a private company giving them an overview of the obligations that companies are subject to in relation to data protection under the GDPR from May 2018 onwards. It provides a broad overview of the areas that need to be addressed internally within the company to ensure on-going compliance and the need for the company to have in place a company-wide regime to ensure compliance with the GDPR.

Compliance should include amongst other things:

- staff training;
- carrying out a data protection audit, assessing the current state of play within the business, determining the degree to which current practices align with the requirements set down in the GDPR and identifying areas for improvement;
- implementing a GDPR data protection policy; and
- implementing relevant GDPR compliant privacy policies.

Simply-Docs' GDPR and Data Protection templates can be accessed here. Demonstrating GDPR compliance should help enhance organisations' public image as consumers and customers will have confidence in how their personal data is handled.

1. Introduction – what is the GDPR?

The GDPR is an EU wide Regulation and in the UK it replaces the Data Protection Act 1998 (DPA 1998). It contains some onerous obligations and will have more of an impact on some organisations than on others. The sanctions for breaches are significantly higher than under the DPA 1998 and whilst there is no direct personal liability for directors set out in the GDPR, given the levels of potential fines and reputational harm to a business, a board's failure to ensure the protection of personal data may be considered a failure by a director to promote the success of the company (s.172 Companies Act 2006). It may also be seen as a failure to exercise reasonable care, skill and diligence, which could result in an action for damages against an individual director and/or their termination or disqualification from office.

2. GDPR Financial Penalties

The GDPR establishes a tiered approach to penalties for breaches. Fines can be imposed for infringements of up to 4% of annual worldwide turnover or EU€20 million, whichever is the higher.

3. Personal Data

The aim of the GDPR is to ensure good information handling practice. An individual has a fundamental right in the UK (and across the European Economic Area (EEA)) to have their personal data protected. Personal data may only be processed, i.e. obtained, recorded, held, used or disclosed, under certain circumstances.

Personal data is a very valuable business asset which includes data relating to any living individual who can be identified from that data. This includes names, addresses, social security numbers, telephone numbers, health information, employee information etc. A wider range of data is classed as "personal data" under the GDPR than under the DPA 1998. It now includes widely-used data such as IP

© Simply-Docs - CO.DCL.08 - GDPR Memo to Board of Directors

addresses and mobile device IDs. In some cases, even data that has been pseudonymised (key-coded, for example) can still qualify if the pseudonym can be tied to a particular person. Generally, if the Board is unsure whether the information it has stored is personal data, it is best to err on the side of caution. This means not only making sure data is secure, but also ensuring that it isn't stored for any longer than necessary.

Businesses will need to know what personal data they hold, where it came from, where it is stored, what it is being used for, who it is shared with and how secure it is. There must be a clear lawful basis for collecting, holding and processing data. This may be that the data subject has given his/her consent to the processing of his/her personal data for one or more specific purposes. Boards should note that the processing of data is lawful only if and to the extent that at least one of the provisions in Article 6 of the GDPR applies. As well as consent, Article 6 lists the other lawful bases for processing data. This includes being necessary for the performance of a contract to which the data subject is party or for compliance with a legal obligation. The full list is set out in Article 6.

This should all be documented. Doing this will help a business to comply with the GDPR's accountability principle which requires organisations to be able to show how they are complying with the data protection principles (Article 5 of the GDPR), for example by having policies and procedures in place so that they can effectively achieve the right balance between the risks and opportunities that using personal data brings.

Article 5 lists the core principles relating to the processing of personal data. Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data.

4. The Board

As mentioned above, board members do not have personal liability for breaches under the GDPR, however a failure to protect personal data will have both personal consequences for directors and for the business. It may be claimed that a director has failed in their Companies Act 2006 duties and businesses may face punishing fines, adverse publicity, civil and potentially even criminal liability.

The Board has a duty to know about the content and operation of its compliance programme and to oversee its implementation. To ensure the accountability principle is adhered to on an on-going basis, the Board will need to understand and make sure the business is correctly implementing its privacy policy and related policies and procedures and is lawfully processing data. The Board should ensure that a" privacy by design" approach is taken to all projects involving personal data.

The Board should also understand the enhanced rights of the individual under the

© Simply-Docs - CO.DCL.08 - GDPR Memo to Board of Directors

GDPR, including greater transparency and the “right to be forgotten”. Individual’s consent (where consent is relied upon as a lawful basis for the use of personal data) to processing personal data must also be based on clear affirmative action, be freely given, specific, informed and unambiguous. There must be a positive “opt-in” which cannot be conferred from silence, pre-ticked boxes or inactivity. Requests for consent should be separate from other terms and be in clear and plain language. This must all be implemented correctly and in a timely manner.

The Board should also ensure that the business is in a position at all times to respond quickly to any data subject’s request, such as requests for a copy of all personal data held by the business on an individual or to erase or rectify all such personal data.

5. Data Protection Officer (DPO)

All public sector organisations must appoint a DPO. Most SME businesses are not required to appoint a DPO, only organisations that carry out large-scale systematic monitoring of individuals (e.g. online behaviour tracking) or large-scale processing of special categories of data (also known as “sensitive personal data”) or data relating to criminal convictions and offences.

However, many businesses may still appoint a DPO to oversee compliance and awareness within the business. Irrespective of whether a DPO is appointed, the legal obligations imposed on your business by the GDPR remain the same. The business therefore may wish to consider appointing a DPO who can report to the Board and provide the relevant on-going knowledge, expertise and day to day commitment to properly advise on how to conduct compliance activities in relation to the GDPR. For those businesses with a DPO already in place, make sure that the person knows and understands the role as required under the GDPR and is able to take proper responsibility for data protection compliance and has the knowledge, support and authority to carry out their role effectively.

6. Organisational Culture

Businesses must display an organisational culture that encourages compliance with the GDPR and provide staff with the guidance and tools they need to achieve this. It should come from the top down.

At the very least there should be a member of staff responsible for data protection compliance, and senior staff members should also be aware of the business’s obligations under the legislation and of data subjects’ rights. Data protection training should be undertaken for all staff whose work involves personal data, however senior staff would be well advised to have a more detailed understanding of how the law affects their business as a whole.

In addition to overall awareness, it is important that this translates into a proactive approach to data protection within the whole business. Consider whether regular meetings between senior staff, particularly those with responsibility for data protection matters, would improve your compliance.

The GDPR also requires businesses to notify the supervisory authority of all data breaches without undue delay and where feasible within 72 hours. Businesses will need robust data breach plans and a procedure in place in the event that such a breach occurs.

© Simply-Docs - CO.DCL.08 - GDPR Memo to Board of Directors

7. Resources and Training

Businesses should put aside sufficient resources - financial, technological and in terms of human resources - to promote compliance with the GDPR. This should include effective compliance staff training programmes for staff of all levels.

This memo should act as the beginning of the Board's GDPR journey. Our GDPR templates aim to help you and your business navigate its implementation and on-going compliance **[**and specifically our GDPR Data Protection Policy[1]**]**.

[1] This document is available to download from our Business Folder.

© Simply-Docs - CO.DCL.08 - GDPR Memo to Board of Directors