M rs:
General Data ulation (GDPR)

This is the type of memo that can of a private company giving them an overview of the obligations th ct to in relation to data protection under the GDPR from May 2018 broad overview of the areas that need to be addressed internally w sure on-going compliance and the need for the company to have in egime to ensure compliance with the GDPR.

Compliance should include among

- staff training;
- carrying out a data protec e current state of play within the business, determining th urrent practices align with the requirements set down in t areas for improvement;
- implementing a GDPR data
- implementing relevant GD cies.

Simply-Docs' GDPR and Data Pr be accessed here. Demonstrating GDPR compliance should help public image as consumers and customers will have confidence in s handled.

1. Introduction – what is th

The GDPR is an EU wide UK it replaces the Data Protection Act 1998 (DPA 1998). It co ligations and will have more of an impact on some organisa The sanctions for breaches are significantly higher than u whilst there is no direct personal liability for directors set o the levels of potential fines and reputational harm to a busi ensure the protection of personal data may be considered to promote the success of the company (s.172 Companie be seen as a failure to exercise reasonable care, skill and result in an action for damages against an individual direct n or disqualification from office.

2. GDPR Financial Penalties

The GDPR establishes a alties for breaches. Fines can be imposed for infringements rldwide turnover or EU€20 million, whichever is the higher.

3. Personal Data

The aim of the GDPR is t n handling practice. An individual has a fundamental right in European Economic Area (EEA)) to have their personal da data may only be processed, i.e. obtained, recorded, held, u certain circumstances.

Personal data is a very va hich includes data relating to any living individual who ca at data. This includes names, addresses, social securi numbers, health information, employee information etc. classed as "personal data" under the GDPR than under the des widely-used data such as IP

addresses and mobile d ases, even data that has been pseudonymised (key-code qualify if the pseudonym can be tied to a particular person. s unsure whether the information it has stored is personal dat e side of caution. This means not only making sure data is s g that it isn't stored for any longer than necessary.

Businesses will need to k a they hold, where it came from, where it is stored, what it is s shared with and how secure it is. There must be a clear law holding and processing data. This may be that the data subj nsent to the processing of his/her personal data for one or es. Boards should note that the processing of data is lawfu that at least one of the provisions in Article 6 of the GDPR a ent, Article 6 lists the other lawful bases for processing data cessary for the performance of a contract to which the data ompliance with a legal obligation. The full list is set out in Art

This should all be docum lp a business to comply with the GDPR's accountability prin anisations to be able to show how they are complying with t ples (Article 5 of the GDPR), for example by having polici lace so that they can effectively achieve the right balance opportunities that using personal data brings.

Article 5 lists the core princ essing of personal data. Personal data shall be:

- processed lawfully, ent manner in relation to the data subject;
- collected for spec mate purposes and not further processed in a mar with those purposes;
- adequate, relevan is necessary in relation to the purposes for which
- accurate and, wher date;
- kept in a form whic f data subjects for no longer than is necessary for the sonal data are processed; and
- processed in a mar riate security of the personal data.

4. The Board

As mentioned above, boa ve personal liability for breaches under the GDPR, howeve sonal data will have both personal consequences for director It may be claimed that a director has failed in their Compa d businesses may face punishing fines, adverse publicity, civ iminal liability.

The Board has a duty to and operation of its compliance programme and to oversee ensure the accountability principle is adhered to on an on-goi eed to understand and make sure the business is correctly policy and related policies and procedures and is lawfully oard should ensure that a" privacy by design" approach is tak g personal data.

The Board should also ur rights of the individual under the

GDPR, including greater ight to be forgotten". Individual's consent (where consent is basis for the use of personal data) to processing personal dat clear affirmative action, be freely given, specific, informed a must be a positive "opt-in" which cannot be conferred from s or inactivity. Requests for consent should be separate from c ar and plain language. This must all be implemented correct .

The Board should also e s is in a position at all times to respond quickly to any da uch as requests for a copy of all personal data held by the ual or to erase or rectify all such personal data.

5. Data Protection Officer (D

All public sector organisat O. Most SME businesses are not required to appoint a DPO t carry out large-scale systematic monitoring of individuals (e king) or large-scale processing of special categories of data e personal data") or data relating to criminal convictions and

However, many business DPO to oversee compliance and awareness within the busi ther a DPO is appointed, the legal obligations imposed on yo R remain the same. The business therefore may wish to con who can report to the Board and provide the relevant on-go e and day to day commitment to properly advise on how to vities in relation to the GDPR. For those businesses with a D e sure that the person knows and understands the role as PR and is able to take proper responsibility for data pro has the knowledge, support and authority to carry out their

6. Organisational Culture

Businesses must display a that encourages compliance with the GDPR and provide sta tools they need to achieve this. It should come from the top o

At the very least there sh aff responsible for data protection compliance, and senior s lso be aware of the business's obligations under the legis cts' rights. Data protection training should be undertaken for a ves personal data, however senior staff would be well advise ed understanding of how the law affects their business as a

In addition to overall awa at this translates into a proactive approach to data protecti siness. Consider whether regular meetings between senio se with responsibility for data protection matters, would i

The GDPR also requires supervisory authority of all data breaches without undue d within 72 hours. Businesses will need robust data breach n place in the event that such a breach occurs.

7. Resources and Training

Businesses should put as - financial, technological and in terms of human resource nce with the GDPR. This should include effective complianc nes for staff of all levels.

This memo should act as the begi PR journey. Our GDPR templates aim to help you and your busine ntation and on-going compliance [and specifically our GDPR Data P

[1] This document is available to download from our