Simplifying Compliance

P4P Compliance Management Limited

UK Data Protection Laws 2024

Data Protection and Digital Information Bill

Table of Contents

© 2023 P4P Compliance Management Limited

Introduction

This article has been produced to give an overview of the proposed UK General Data Protection Regulation (UK- GDPR) replacement – The Data Protection and Digital Information Bill (DPDI) to help organisations and individuals understand the anticipated new legal data protection framework in the United Kingdom.

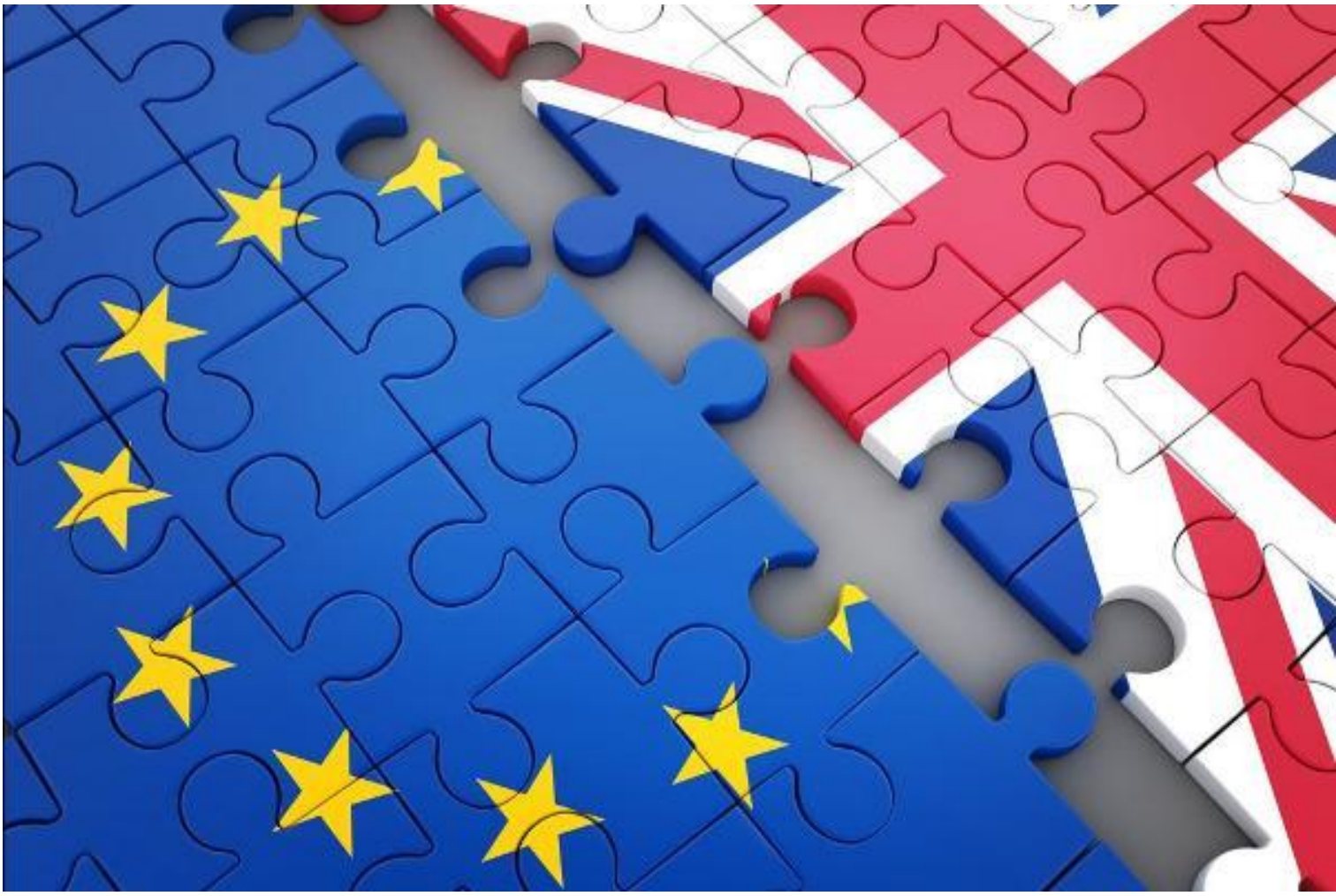
As it currently stands, the DPDI doesn't completely replace the existing UK-GDPR legislation but amends the current version along with the Data Protection Act 2018 (DPA 2018).
The reasoning being that the UK Government wanting to preserve the adequacy decision with the EU, whilst trying to reduce the regulatory burden on UK businesses.

The new bill cross references, the UK-GDPR, DPA 2018, the DPDI Explanatory Notes and Data Protection Impact Assessment (DPIA).

In this article, we've aimed to explain in simple terminology (no elaborate jargon) the proposed key features of the DPDI and describe some potential new challenges businesses face in 2024 complying with new proposed data protection rules.

© 2023 P4P Compliance Management Limited

Post-Brexit GDPR



1st January 2021 the UK formally left the European Union (EU) and became known as a third country.

This led to the creation of EU-GDPR and the Data Protection Act (2018) UK-GDPR The new UK-GDPR is identical to the EU-GDPR but is an independent UK legislation governed and enforced by the UK data protection agency Information Commissioner's Office (ICO) and does not influence EU authorities.

Based on the same legal language as the EU-GDPR, it replaced EU and Union law context with UK and domestic law and has the same GDPR principles, rights, and obligations. However, there are implications for the rules on transfers of personal data between the UK and the European Economic Area (EEA).

© 2023 P4P Compliance Management Limited

New Data Protection Bill

Introduced in the House of Commons 18 July 2022 (Bill 143) was intended to harness UK's post-Brexit freedoms to create an independent data protection framework.

The Bill was paused in September 2022 for ministers to collaborate with business advisory groups and data experts in the redesign of UK data protection rules.

08 March 2023 the UK Government decided to propose a new version of UK-GDPR (Post Brexit) data law, using current high standards for data protection and privacy, and move away from the 'one-size-fits-all' European Union's GDPR model.

Formally known as The Data Reform Bill, The DPDI Bill aims to reduce the number of repetitive data collection cookie pops-ups online, remove barriers to international trade, and lower costs and responsibilities for British businesses and charities.

The new bill proposes to:

- Be less complicated, clearer, and have a more business-friendly framework.
- Cut down on needless paperwork, organisations need to demonstrate compliance.
- Take the best bits of current UK-GDPR to give businesses more flexibility in the way they comply with data laws.
- Give organisations greater confidence about when they can process personal data without consent.
- Maintain data adequacy with the EU, and wider international confidence in the UK's comprehensive data protection standards.
- Support more international trade without creating extra costs for businesses if they're already compliant with current data regulation.
- Support more international trade for businesses if they're already compliant with current data regulation so they don't incur extra unnecessary costs
- Increase public and business confidence in Artificial Intelligence (AI) technologies. Currently you "normally" need to tell individuals what information you hold about them and how it is being used when using AI to process someone's personal data.

© 2023 P4P Compliance Management Limited

What Does the DPDI Mean?

For UK businesses the DPDI Bill (No 2) pledges to maintain a high standard of data protection rights, so businesses can expect strict data protection compliance rules.

However, DPDI proposes to offer businesses more flexibility in how they manage record keeping, and proposed changes to online cookies, such as allowing for the use of certain analytical cookies without consent where the data is being used to improve online services and websites.

Businesses will need to check that their current standards and internal processes and procedures meet the proposed new requirements established by DPDI.
They need to consider the proposed requirements of DPDI Bill (No 2) carefully and understand the differences from the current UK-GDPR, and Data Protection Act 2018 along with the Privacy and Electronic Communications (EC Directive) 2003 to be compliant with the new regime.

The proposed DPDI Bill could introduce many changes in the way businesses practically collect and process personal data, potentially including:

- **Flexibility in Accountability**
  The DPDI implies that there is no longer a requirement for businesses to appoint a Data Protection Officer (DPO) or Data Protection Impact Assessment (DPIA) to identify risks arising out of the processing of personal data.
  However, management and mitigation of data risks will still be a major requirement for compliance.

- **Relying on legitimate interests**
  In practice, this could mean that businesses could rely on legitimate (justifiable) interests as a lawful way for processing personal data in certain circumstances.

- **Data Subject Access Requests (DSARs)**
  Organisations could potentially decide to refuse DSARs if they determine them to be “vexatious (troublesome) or excessive (unnecessary)”.
  This aligns with the Freedom of Information (“FOI”) regime and clarifies the vague concept of “manifestly (clearly) unfounded or excessive”.

- **Information Commissioner Office (ICO)** increased fines under **Privacy and Electronic Communications Regulations (PECR)**
  Possible increase penalties for businesses that engage in unsolicited marketing calls and electronic communications.

- **Removal of website(s) Cookie Consent**
  PECR could be amended, so that cookie consent is no longer a requirement when used purely for website analytics.

© 2023 P4P Compliance Management Limited

Will DPDI be Easier than GDPR?

Whilst the DPDI Bill intends to reduce the compliance burden on UK businesses and move away from the EU-GDPR rules, it doesn't look like fundamental changes.

Currently the UK-GDPR adequacy decision allows for the free flow of data to the EU without organisations having to put any additional measures in place.

The UK Government must consider balancing easing data protection compliance for UK businesses, against the risks of making changes to the current adequacy decision. The major risk being EU businesses perceiving that EU personal data under the new Bill may no longer be adequately protected in the UK, impacting EU trading with the UK.

© 2023 P4P Compliance Management Limited

Current UK-GDPR v DPDI Bill v2.0

Some of the main proposed changes listed in the table below

Current Position	Proposed DPDI Bill v2.0	Summary
Definition of Personal Data		
Personal data is defined as “any information relating to an identified or identifiable natural person”. Anyone who can be identified directly or indirectly. **Article 4 UK-GDPR**	Personal data definition has been amended in an attempt to clarify the process for determining if information relates to an individual who is “identifiable”. Information being processed will only be deemed to be information relating to an identifiable individual: 1) Where the individual is identifiable by the controller or processor by reasonable means at the time of processing 2) Where the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing and the individual will be, or is likely to be, identifiable by that person by reasonable means at the time of processing. **Clause 1 DPDI**	The revised definition restricts the assessment in two ways: 1) It is limited to identification by the controller, processor or any third party, who is likely to receive the information, rather than the public. 2) Identification only needs to be by “reasonable means”. This is likely to be broadly welcomed, particularly by organisations that want to anonymise data.
Purpose Limitation		
Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes. Certain factors to be considered when determining if a purpose is incompatible	Specific provisions have been added to assist controllers when determining if a new purpose is compatible with the original purpose. Factors to be considered: 1) The context in which the personal data was collected, including the	This amendment provides clarification of the change to the existing requirements.

© 2023 P4P Compliance Management Limited

include the nature of the personal data and the context in which it was first collected. **Articles 5-6 UK-GDPR**	relationship between the controller and data subject 2) The nature of the personal data and 3) The consequences of the intended processing. A specific list of purposes judged to be compatible is provided which includes any processing carried out to ensure compliance with the lawful, fair, and transparent. **Clause 6 DPDI**	
Legitimate Interests		
When relying on legitimate interests as a lawful basis, controllers must perform a legitimate interest's assessment (LIA) to help them decide whether the legitimate interests in processing personal data outweigh the rights of data subject(s). Controllers may rely on consent as lawful basis, rather than making a wrong decision, that would be detrimental to the data subject(s). **Article 6(1) UK-GDPR**	The Bill creates a new lawful ground for processing personal data, allowing organisations to process personal data where necessary for a "recognised legitimate interest" such as preventing crime, civil emergencies, and safeguarding vulnerable individuals in a new Annex 1 to the UK-GDPR. **Clause 5 DPDI**	The Bill sets out examples of activities which will fall within the "legitimate interest" condition. These include processing for direct marketing, within a group, especially within a social group (intragroup) transfer, and for network security.
Data Subject Access Request (DSAR)		
The current Subject Access Request or 'SAR' gives individuals the right to obtain a copy of their personal data, to understand how and why you are using their data, and check you are doing it lawfully. You cannot charge a fee to comply with an SAR, but you can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive.	The Bill amends the exemption so that organisations can refuse to respond to a Data Subject Access Request (DSAR) or charge a fee if a DSAR is 'vexatious (mischievous), not made in good faith or is an abuse of process. **Clause 7 DPDI**	This exemption will allow more DSARs to be refused than the existing exemption of 'manifestly (deliberately) unfounded or excessive'.

© 2023 P4P Compliance Management Limited

If you refuse to comply with a request, you must inform the individual of: 1) The reasons why 2) Their right to make a complaint to the ICO or another supervisory authority. 3) Their ability to seek to enforce this right through the courts. **Article 12 UK-GDPR**		
Accountability Controllers and Processors		
Controllers and Processors outside the UK must appoint a UK representative in certain circumstances to comply with the UK-GDPR **Article 27 UK-GDPR**	Controllers and Processors outside the UK who currently comply with the UK-GDPR because of the extra-territoriality provisions, will no longer be required to appoint a UK-based representative. The Bill also offers that a controller or processor is exempt from the duty to keep records unless they are carrying out "high risk" processing. **Clause 13 DPDI**	The Bill reduces Controllers and Processors administration while being beneficial for those organisations with cross-border operations as it cuts down on resources and administration.
Accountability Senior Responsible Individual		
Certain organisations are required to appoint a Data Protection Officer (DPO). The DPO assists with monitoring internal compliance, informs, and advises on data protection obligations, provides advice regarding and acts as a point of contact for data subjects and the Information Commissioner. **Articles 37-39 UK GDPR**	The Bill replaces the need to appoint a DPO with a new requirement for a designated Senior Responsible Individual (SRI) who must be part of the organisation's "senior management". **Clause 14 DPDI**	It is likely that the existing role of DPO will be renamed to SRI. This proposed change presents 3 potential problems: 1) The requirement for the SRI to "be part of" the organisation's senior management could impact pay grades, promotions etc. 2) Existing external DPO appointments could be at risk, as the organisation could seek

© 2023 P4P Compliance Management Limited

		to source this role internally 3) Data subjects' protection could be at risk if SRI tasks and responsibilities are delegated to any person carrying them without necessary skills and or experience.
Data Protection Impact Assessments (DPIA)		
A Data Protection Impact Assessments (DPIA) must be carried out where processing of personal data is likely to result in high risk to individuals. If a DPIA results in the identification of a data processing activity that poses high risks that cannot be mitigated, organisations are obligated to consult with the ICO prior to processing any data. **Articles 35-36 UK GDPR**	The requirement to perform a DPIA, has been replaced with now having to carry out an "Assessment of High-Risk Processing". This will require organisations to provide a summary of the purposes of processing, assessment of necessity and risks to individuals and a description of how they intend to mitigate any risks. The mandatory requirement for prior consultation with ICO has been replaced with a voluntary consultation process. **Clause 17-18 DPDI**	The Assessment of High-Risk Processing should give organisations a bit more flexibility, in how they identify managing and mitigate privacy risk.
Automated Decision Making (ADM) and Artificial Intelligence (AI)		
Data subjects have a right to not be subjected to decisions based solely on automated decision making. Where a decision is made, certain specified safeguards must be in place. **Article 22 UK GDPR**	The Bill clarifies that a decision based solely on automated processing (the creation and implementation of technology that automatically processes data), using technology such as computers and other electronic communication to collect, store, manipulate, prepare, and distribute data, where there has been no "meaningful human involvement" in the decision making. The restrictions now only apply where a decision is based on special categories of personal data.	Automated decision making has been clarified to mean a decision where there is "no meaningful human involvement". The Bill limits the restrictions on ADM to those decisions which include special categories of personal data.

© 2023 P4P Compliance Management Limited

	An automated decision may only be made if: 1) The data subject has given consent. 2) The decision is necessary for a contract or required by law and a substantial public interest condition applies. In all cases, certain (enhanced) safeguards must be in place including the right to obtain human intervention and contest decisions. **Clause 11 DPDI**	
Privacy and Electronic Communications Regulations (PECR) 2003		
Consent for the use of cookies is required in all circumstances unless such use is strictly necessary. **Regulation 6 PECR 2003**	The Bill allows businesses to implement cookies without the need for consent, for functionality and statistical purposes i.e. how websites and services are used for improvement purposes, or to update software such as security patches. **Clause 79 DPDI**	This will be beneficial to many businesses who will be able to use analytics cookies on their websites or services without having the visitor's consent. This will provide useful information such as how many people have visited, where they have come from, the pages and content they've spent the most time on.
Direct Marketing and Nuisance Calls		
Fines for making unwanted marketing calls and texts is capped at £500,000 **Regulation 6 PECR 2003**	Fines for nuisance calls and texts are to be increased and align with GDPR from £500,000 to either 4% of global turnover or £17.5 million, whichever is greater. **Clause 86 DPDI**	Consumers plagued by nuisance calls and texts will benefit from the changes to the law, so those firms can no longer escaped punishment and be hit with substantial fines.

© 2023 P4P Compliance Management Limited

What to do Now?

All UK organisations should maintain compliance with UK-GDPR laws until the UK Government announces the change in the Data Protection law.

Types of Data Breaches

Personal Data Breach
A breach is more than just losing personal data it's a breach of security that leads to the accidental or unlawful (deliberate) destruction, loss, alteration, unauthorised disclosure of or access to personal data.
An organisation must report certain personal data breaches to the ICO where possible within 72 hours of becoming aware of the breach.
You must also inform those individuals without undue delay if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.
You must keep a record of any personal data breaches.

Privacy and Electronic Communications Regulations (PECR)
This is a security breach by a telecoms or internet service provider
Service providers must notify the ICO that a personal data breach has occurred within 24 hours of becoming aware of the breach.
The service provider must notify individuals without unnecessary delay if the breach is likely to adversely affect individuals.
Service providers must keep a log of any breaches and submit to the ICO on a monthly basis.
If the personal data was encrypted to an appropriate standard and remains secure, service providers should still notify the ICO of the breach.

Network and Information Systems (NIS)
NIS concerns the security of network and information systems and the digital data contained within them.
NIS only applies to Operators of essential services (OES) and Relevant digital service providers (RDSP)
NIS requires OES and RDSPs to notify their competent authorities if an incident occurs.
Where an incident is, or becomes, a personal data breach, organisations also need to inform the ICO separately.

Electronic Identification and Trust Services
EIDAS Regulations set the rules for the identity of individuals and businesses online and verifying the authenticity of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.
A breach of security or loss of integrity that has a significant impact on a trust service provided or on the personal data held therein.
A deliberate attack can cause a breach, compromising the integrity of the service.
A breach can also occur if there is an unauthorised access within an organisation or an accidental loss of integrity.

© 2023 P4P Compliance Management Limited

Breach reporting rules are detailed in UK EIDAS Regulation Article 19.
An organisation will need to notify the ICO and their users and inform anyone else who might be affected.

Data Breach Reporting

A data breach can be any incident that results in the accidental or unlawful (deliberate) destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data breaches can be the result of a criminal hacker breaking into your systems, when an employee accidentally sends personal information to the wrong person, loses a laptop containing personal data or fails to password-protect an online database.
All these scenarios are subject to the GDPR data breach reporting requirements and require you to report data breaches to your organisations supervisory authority.
For UK organisations this is the ICO and you must notify them of a data breach within 72 hours of becoming aware of it.

ICO can offer advice about what to do next, how to contain it, and how to stop it happening again.

Where a significant cyber incident occurs, you may also need to report this to the National Cyber Security Centre (the NCSC).

Mitigating the Risk

5 top recommendations to safeguard against data breaches and mitigate the risk of non-compliance

1. Conduct regular Data Protection Impact Assessments (DPIAs)
   Identify, assess, and mitigate privacy risks to data processing activities, especially when introducing new data processes, systems and technologies.

2. Implement processes and procedures to ensure governance of client, employee, and others personal data you obtain and store.

3. Staff training and awareness
   Educate and keep your people up to date with GDPR, what it is and when it needs to be applied.

4. Prepare for phishing attacks in which a perpetrator poses as a trustworthy source and attempts to trick people into clicking malicious links delivered by emails.

5. Back up your data. Cyber attackers generally just steal information, but can hold you to ransomware (malware that employs encryption to hold a victim's information at ransom).

© 2023 P4P Compliance Management Limited

Conclusion

Businesses globally have had to survive the past few turbulent years getting through the Coronavirus pandemic and still face huge challenges with the aftermath, and economic crisis.

Organisations that have allowed employees to continue to work from home or have outsourced work previously done by staff they let go due to save costs, now face extra worries with data protection.

In 2024 many businesses will have to rethink and change their ways of working, develop new strategies, and become more digital, to avoid fines for non-compliance with predicted changes in data protection laws.

Individuals are more empowered and aware of their rights as the GDPR enhances transparency and gives individuals enforceable rights, such as the right of access, rectification, erasure, the right to object and the right to data portability. Individuals also have the right to make a complaint with a data protection authority and to seek an effective judicial remedy.

GDPR has provided organisations a single set of rules and a harmonised framework for the protection of personal data.

Compliance with the data protection rules will create trust between business and consumers when it comes to the use of their personal data.

Image Credits

Cover image by rawpixel.com
Post-Brexit GDPR - free stock / CC0 licenced.
Will DPDI be easier than GDPR? image by Kues

Disclaimer

P4P Compliance Management Limited work very hard to provide up-to-date accurate information through thorough research at the time of publishing; however, some information may understandably be less accurate as time passes. We make no representations or warranties of any kind (expressed or implied) about the completeness, accuracy, reliability, suitability or availability of any information, products, services, or related graphics contained in this article.
All images used in this article are purchased, free stock, or CC0 licenced and accredited to the artist where possible.

© 2023 P4P Compliance Management Limited