The UK Data Protection and Digital Information Bill

A practical comparative analysis with the EU GDPR and ePrivacy framework

By the Hogan Lovells U.K. Privacy and Cybersecurity team

On July 18, 2022, the U.K. government introduced the Data Protection and Digital Information Bill to Parliament. Previously known as the Data Reform Bill, it is the result of a consultation from 2021 and its aim is to update and simplify the U.K.'s data protection framework. According to the U.K. government, the new legal framework created by the DPDI Bill will reduce burdens on organizations while maintaining high data protection standards.

Given that the current U.K. data protection framework essentially mirrors the EU General Data Protection Regulation and EU ePrivacy framework, this comparative analysis considers the changes proposed by the DPDI Bill by reference to the relevant EU law provisions and addresses the following practical questions:

- Whether the U.K. approach is more or less onerous than the EU provision.
- Whether applying the EU interpretation in the U.K. will be compliant.
- Whether there is an advantage in relying on the U.K. approach.

Taking these factors into account, the proposed legislative changes are color-coded in the table below as follows:

Positive impact for ease of compliance	Neutral impact for ease of compliance	Negative impact for ease of compliance

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
EU GDPR		
Definitions		
Article 4 and Recital 26 (Definition of personal data) The EU GDPR applies to 'personal data.' Personal data is defined as any information relating to an 'identified or identifiable' individual. An identifiable individual is one who can be identified directly or indirectly. To determine whether an individual is indirectly identifiable, account should be taken of all the means 'reasonably likely' to be used, such as singling out, either by the controller or by another person. Anonymous data is data that is not related to an identified or identifiable natural person, and is not in scope of the Regulation.	**Clause 1(3) (Definition of personal data)** The DPDI Bill retains the same basic definition. However, it further clarifies when data is related to an identified or identifiable individual and when it should be considered anonymous. Information will only be considered as identifiable by a person other than the controller or processor if that other person will, or is likely to, obtain the information as a result of the processing. If they are not or are not likely to obtain the information, this will be considered anonymous information.	→ The U.K. approach reduces uncertainty as to when data is anonymized in a manner which is likely to benefit the controller. → Applying the EU interpretation in the U.K. will be compliant. → Marginal advantage in relying on the U.K. approach.
Article 4 and Recitals 159, 160, 162 (Definition of research and statistical purposes) The EU GDPR contains various exemptions where personal data is being processed for scientific or historical research purposes or statistical purposes. However, these terms are not defined in the body of the EU GDPR. Instead, recitals 159, 160 and 162 contain interpretive guidance. For example, recital 159 states that scientific research should be interpreted in a broad manner, and provides examples of technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health.	**Clause 2 (Definition of research and statistical purposes)** The DPDI Bill moves much of the interpretative guidance from the recitals into the main body of the U.K. GDPR. The interpretations remain broadly similar, although there are some helpful clarifications, such as that scientific research means 'any research that can reasonably be described a scientific, whether publicly or privately funded'.	→ The U.K. approach is similar but may reduce uncertainty in a way which is beneficial to controllers processing personal data for scientific research purposes. → Applying the EU interpretation in the U.K. will generally be compliant. → Marginal advantage in relying on the U.K. approach.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Definitions		
Article 4 and Recital 33 (Consent for scientific research) The EU GDPR requires that where consent is relied on as the lawful basis for processing, the consent must be given for a specific purpose of processing. This can cause challenges in the context of exploratory scientific research, where it may not be possible to fully identify the objective of the research at the outset. The main body of the EU GDPR does not provide a solution to this, although recital 33 notes that individuals should be allowed to consent to areas of research where in keeping with recognized ethical standards, and when individuals are given the option of consenting only to part of the research where practical.	**Clause 3 (Consent for scientific research)** The DPDI Bill moves the substance of the recital into the body of the U.K. GDPR but does not substantively alter its meaning.	→ The U.K. approach provides legal certainty but does not alter the intent of the existing EU recital. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach provides additional legal certainty.
Principles and lawful grounds of processing		
Article 6(1)(e) and (f) (Lawfulness of processing) The EU GDPR requires that all processing has a lawful ground. One of these lawful grounds is that the processing is necessary for the purposes of the legitimate interests of the controller or a third party, and those interests are not overridden by the interests or fundamental rights of the data subject. Relying on this lawful ground requires conducting a balancing test on a case-by-case basis. An alternative legal basis is where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	**Clause 5 and Schedule 1, Annex 1 (Lawfulness of processing)** The DPDI Bill removes the need to assess whether processing for certain 'recognised' legitimate interests is overridden by the interests or rights of the data subject. These 'recognized' legitimate interests are laid out in Annex 1. A procedure is set out for the U.K. government to add to this list in the future. The current list focuses on 'public interests' such as national security, public security, defense, emergencies, preventing crime, safeguarding and democratic engagement.	→ The U.K. approach removes the requirement to conduct a balancing test when processing for a legitimate interest specified in Annex 1. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach makes it simpler to process data for recognized legitimate interests.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Principles and lawful grounds of processing		
Article 5(1)(b) and Article 6 (Purpose limitation principle) The EU GDPR requires that personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ('purpose limitation' principle). The EU GDPR sets out factors to consider when determining whether processing for a new purpose is 'compatible' with the initial purpose. It also states that further processing for purposes of archiving in the public interest, scientific or historical research, or statistics will not be considered incompatible with the original purpose.	**Clause 6 and Schedule 2, Annex 2 (Purpose limitation principle)** The DPDI Bill maintains a similar general test for determining whether processing for a new purpose is 'compatible.' However, it introduces a list of additional scenarios where processing for a new purpose will be considered as compatible. The new 'compatible scenarios are laid out in clause 6 and Annex 2. A procedure is set out for the U.K. government to add to this list in future. The current list is extensive and includes processing for research, archiving and statistics, several other 'public interest' purposes as well as, for example, to enable controllers to comply with their legal obligations. The 'compatible purposes' are somewhat restricted when the initial processing is based on consent. The DPBI Bill also clarifies that processing is not lawful simply because it is being carried out for purposes which are compatible with the purposes for which it was collected.	→ The U.K. approach reduces uncertainty in a way which is mostly beneficial to controllers. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach makes it simpler to comply with the purpose limitation principle.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Data subject rights		
Article 12 and Articles 15-22 (Vexatious or excessive requests and time limits for responding) The EU GDPR provides data subjects with certain rights exercisable against controllers, including the right of access, right to rectification, right to erasure, the right to restrict processing, right to data portability and right to object. Requests cannot be refused unless the controller can demonstrate it is not in a position to identify the data subject or if the request is manifestly unfounded or excessive. The EU GDPR states that this may be the case in particular because of their repetitive character but does not explicitly define these terms. Controllers have one month from receipt of the request to respond substantively, although this may be extended by two further months where necessary, taking into account the complexity and number of requests.	**Clause 7 and Clause 8 (Vexatious or excessive requests and time limits for responding)** The DPDI Bill replaces the EU GDPR's 'manifestly unfounded or excessive' threshold for refusing requests with a new 'vexatious or excessive' threshold. The DPDI Bill outlines several factors to be considered when determining whether requests meet this threshold, together with examples of requests which may do so. Among other things, controllers will now be able to take into account their resources and may be able to refuse requests intended to cause distress, not made in good faith, or which are an abuse of process. The DPDI Bill also clarifies that the time period for responding to a request does not run whilst waiting for a requestor to confirm their identity (if requested), provide any reasonably necessary clarifications requested by the controller, or to pay any fees due.	→ The U.K. approach expands the circumstances under which a request may be refused and provides helpful clarity that the clock does not continue to run whilst waiting for the requestor to provide any necessary information that is requested. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach makes it simpler to comply with individuals' rights.
Article 13 and Article 14 (Information to be provided to data subjects) The EU GDPR requires controllers to provide certain transparency information to the data subject. There are certain exemptions to this requirement. In particular, where personal data has not been obtained directly from the data subject, it is not necessary to provide the information where it would (a) be impossible, (b) involve disproportionate effort, or (c) undermine the objectives of the processing. Instead, it is sufficient to take appropriate steps to protect the data subject, which must include making the information publicly available (for example via a privacy notice).	**Clause 9 (Information to be provided to data subjects)** The DPDI Bill expands this exemption such that it also applies to processing personal data which has been collected directly from the data subject for research, archiving or statistical purposes only, where providing such information would be impossible or require disproportionate effort.	→ The U.K. approach makes it less onerous to comply with transparency obligations when processing personal data collected directly from the data subject for research, archiving or statistical purposes only. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach is simpler to comply with when processing personal data collected directly from the data subject for research, archiving or statistical purposes only.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Data subject rights		
Article 22 (Automated decision-making) The EU GDPR provides data subjects with a right not to be subject to decisions based solely on automated decision-making, including profiling, which have legal or similarly significant effects, but this is subject to certain exemptions. A controller carrying out solely automated decision-making under this provision must also implement certain measures to safeguard the data subject, such as providing the right to obtain human intervention.	**Clause 11 (Automated decision-making)** The DPDI Bill substitutes the whole of Article 22 with a new provision by which processing based solely on automated decision-making is only restricted and subject to certain conditions where it involves the processing of special category data. The safeguards that apply to solely automated decision-making have been clarified and arguably expanded, to include an obligation for controllers to provide the data subject with information about the decisions. Measures also must be put in place to enable the data subject to make representations about the decisions, obtain human intervention and contest the decisions. The definition of solely automated is also clarified to mean decision making that involves no meaningful human involvement.	→ The U.K. approach relaxes the restrictions on the use of solely automated decision-making but makes the safeguards that apply to data subjects more explicit. → The EU approach would be broadly compliant in the U.K., although organizations will need to consider whether they are providing sufficient information to data subjects about solely automated decisions. → The U.K. approach makes it marginally simpler to comply with the rules on solely automated decision-making.
Accountability		
Article 24, Article 25 and Article 28 (General obligation relating to technical and organizational measures) Under the EU GDPR, controllers and processors have certain accountability obligations when processing personal data. Controllers must implement appropriate technical and organizational measures to demonstrate their compliance with EU GDPR and must only use processors that provide sufficient guarantees to implement appropriate technical and organizational measures.	**Clause 12 (General obligations)** The DPDI Bill makes a minor amendment to these provisions to require 'appropriate measures, including technical and organizational measures,' rather than merely 'appropriate technical and organizational measures.'	→ The explanatory notes suggest this change is intended to give controllers more flexibility as to the measures they put in place. As drafted however, the new language suggests that the new measures must still include technical and organizational measures. → The EU approach would be broadly compliant in the U.K. → The U.K. approach is intended to allow for greater flexibility, although it is unclear that the current language achieves this.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Accountability		
Article 27 (Representatives for controllers or processors not established in the EU) The EU GDPR requires controllers and processors that are not established in the EU to appoint an EU representative in certain circumstances.	**Clause 13 (Removal of requirement for representatives for controllers or processors outside the U.K.)** The DPDI Bill removes the requirement for controllers and processors not established in the U.K. to appoint a U.K. representative.	→ The U.K. approach is less onerous than the EU position. → Applying the EU interpretation in the U.K. will be compliant (but unnecessary). → The U.K. approach significantly simplifies compliance.
Article 30 (Records of processing activities) The EU GDPR requires controllers and processors to keep a record of their processing activities. For controllers, the records must include the name and contact details of the controller, the purpose of processing, the categories of the data and data subjects, the recipients of the data, any transfers to a third country or international organization, (where possible) the retention of the data and (where possible) the security measures implemented. Processors are subject to a more limited set of record keeping obligations. There is an exemption for organizations of under 250 persons, but only where the processing is not likely to result in a high risk, is not occasional, and does not include special category data or criminal data.	**Clause 15 (Duty to keep records)** The DPDI Bill maintains the obligation for controllers and processors to keep a record of processing which is broadly similar to that required under the EU GDPR. However, the exemption from record-keeping requirements has been expanded, such that it applies to any organization with less than 250 persons which does not conduct high-risk processing.	→ The U.K. approach largely maintains the obligation to keep records of processing, although it may be less onerous for smaller companies not conducting high risk processing. → Applying the EU requirements in the U.K. will broadly be compliant, although the U.K. requirements may require more specificity (for example, an obligation to record who the data has been shared with, rather than merely categories of recipient). → The U.K. approach may be less burdensome for companies with less than 250 employees.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Accountability		
Article 35 (Data protection impact assessment) The EU GDPR requires controllers to carry out a data protection impact assessments where there is high risk processing in relation to new technologies.	**Clause 17 (Assessment of high-risk processing)** The DPDI Bill requires controllers to carry out an assessment of high-risk processing. The assessment needs to include a summary of the purpose, an assessment of whether the processing is necessary for the purpose, an assessment of the risks to individuals, and a description of the proposed mitigations. However, the list of specific circumstances in which a DPIA is considered necessary under the EU GDPR, such as in relation to the processing of large scale special category data, has been removed.	→ The U.K. approach largely maintains the requirement to undertake a DPIA. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach does not lower the standards that trigger the requirement to undertake an assessment of high-risk processing.
Article 36 (Prior consultation) The EU GDPR requires controllers to consult the supervisory authority where the processing has been designated high risk in a DPIA in the absence of measures to mitigate the risk.	**Clause 18 (Consulting the Commissioner prior to processing)** The DPDI Bill makes it optional to consult the Information Commissioner prior to processing that has been designated high risk by an assessment, in the absence of measures to mitigate the risk.	→ The U.K. approach removes this obligation by making regulatory consultation optional. → Applying the EU interpretation in the U.K. will be compliant (but unnecessary). → The U.K. approach significantly simplifies compliance.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Accountability		
Articles 37-39 (Designation, position and tasks of data protection officer) The EU GDPR requires controllers and processors to appoint a data protection officer if the processing is carried out by a public authority, if the processing is on a large scale, or if there are large amounts of special category data being processed. The DPO's tasks involve informing their organization of their processing obligations, monitoring compliance with the data protection legislation, providing advice on data protection impact assessments and acting as the point of contact and cooperating with the supervisory authority.	**Clause 14 (Senior responsible individual)** The DPDI Bill requires controllers and processors to appoint a senior responsible individual if the controller or processor carries out high risk processing or is a public body. Under the DPDI Bill the tasks are different for controllers and processors. The tasks for a controllers' SRI involve monitoring compliance with data protection legislation, ensuring their organization has updated measures to ensure compliance, informing their organization of their processing obligations, organizing training for employees, dealing with complaints on personal data processing, dealing with personal data breaches and acting as the point of contact and cooperating with the Information Commissioner. For a processor, the SRI's tasks involve monitoring compliance and acting as a point of contact and cooperating with the Information Commissioner.	→ The U.K. approach largely maintains the requirement to appoint a DPO, now called SRI. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach does not lower the standards that trigger the appointment of an SRI.
International data transfers		
Articles 44-50 (Transfers of personal data to third countries and international organizations) International transfers of personal data may only take place subject to certain conditions, namely: → The third country ensures an adequate level of protection for the personal data. → In the absence of that adequate level of protection, the controller or processor wishing to transfer the data provides appropriate safeguards. → In the absence of an adequate level of protection or of appropriate safeguards, a transfer fits within one of the derogations for specific situations.	**Clause 21 and Schedule 5 (Transfers of personal data to third countries and international organizations)** The DPDI Bill covers the whole international data transfers regime in a schedule. The Secretary of State may approve transfers of personal data to a third country or international organization through regulations if the so-called 'data protection test' is met, considering factors including the desirability of facilitating transfers of personal data to and from the U.K. Transfers may also be made subject to appropriate safeguards or derogations. However, the Secretary of State may restrict transfers where necessary for important reasons of public interest.	→ The U.K. approach largely maintains the regime dealing with international data transfers, although it provides flexibility for the Secretary of State to approve transfers subject to the data protection test. → Applying the EU interpretation in the U.K. will be compliant subject to specific restrictions introduced by the Secretary of State in the public interest. → The U.K. approach does not necessarily allow greater flexibility in meeting the legal requirements to legitimise international data transfers.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Research safeguards		
Article 89 (Safeguards for processing for research purposes) The EU GDPR contains various exemptions where personal data is being processed for scientific or historical research or statistical purposes. In order to benefit from these exemptions, 'appropriate safeguards' must be applied to the processing. The EU GDPR specifies that these safeguards must ensure respect for the principle of data minimization, for example by pseudonymizing and anonymizing data where possible, but leaves EU member states to further elaborate on what additional safeguards might be necessary.	**Clause 22 (Safeguards for processing for research purposes)** The DPDI Bill maintains the focus on data minimization as a safeguard. It also mirrors existing provisions in the UK Data Protection Act 2018 by specifying that: → The processing must not be likely to cause substantial damage or distress to the data subject. → The processing is not carried out for the purposes of taking measures or making decisions with respect to a particular data subject (except for approved medical research). The DPDI Bill enables the U.K. government to introduce further safeguards.	→ The U.K. approach is more onerous that the EU provision, in that it introduces specific additional safeguards which must be complied with. → Applying the EU interpretation in the U.K. will not alone ensure compliance. → Controllers relying on the research or statistical exemptions in the U.K. will need to ensure they have applied the specified safeguards.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Privacy and Electronic Communications Directive 2002 as amended by Directive 2009/136/EC of the European Parliament and of the Council (ePrivacy Directive)		
Article 5 (Cookies and similar technologies) Organizations are restricted from storing/accessing information, such as cookies and similar technologies, on the terminal equipment of a user unless users have given their consent or the strictly necessary exemption applies.	**Clause 79 (Cookies and similar technologies)** The DPDI Bill introduces an expanded range of exemptions to the consent requirement including: → For the purpose of collecting statistical information about an information society service in order to improve that service. → For enabling the way in which a website appears or functions in order to adapt to the preferences of the user. → For the installation of necessary security updates to software on a device. → To identify the geolocation of an individual in an emergency. For each of these exemptions to apply (other than for emergency geolocation), the user must be provided with clear and comprehensive information and a simple means of objecting.	→ The U.K. approach is generally less onerous than the EU position, allowing cookies and similar technologies to be used for a broader range of purposes without consent. → Applying the EU interpretation in the U.K. will generally be compliant. → The U.K. approach will expand the purposes for which cookies can be used without consent, but requires changes to consent mechanisms and objection processes.
Article 13 (Opt-out exemption) The general rule for the use of electronic mail for direct marketing purposes is prior consent. However, organizations can send electronic marketing communications to customers without prior consent where they obtained the contact details in the context of a previous sale or provision of goods or services, subject to providing them with the right to opt-out.	**Clause 82 (Out-out exemption)** The out-out exemption is being expanded to apply to non-commercial organizations so that they will also be able to send electronic marketing communications without consent for the purposes of furthering charitable, political or other non-commercial objectives, if they obtained the contact details in the course of the individual expressing interest or offering support to the objective.	→ The U.K. approach expands the circumstances under which the out-out exemption can be relied upon. → Applying the EU interpretation in the U.K. will be compliant. → The U.K. approach makes it easier for non-commercial organizations to undertake direct marketing.

cont.

EU Law Provision EU GDPR and ePrivacy Directive	UK Approach Data Protection and Digital Information Bill	Practical Analysis
Privacy and Electronic Communications Directive 2002 as amended by Directive 2009/136/EC of the European Parliament and of the Council (ePrivacy Directive)		
Article 15a (Duty to notify the Commissioner of unlawful direct marketing) The powers of supervision and enforcement are delegated to member states to determine and therefore not specified at an EU-level.	**Clause 85 (Duty to notify the Commissioner of unlawful direct marketing)** The DPDI Bill introduces a duty on providers of public electronic communication services and networks to report to the Information Commissioner suspicious activity relating to unlawful direct marketing. As a consequence, a new power is introduced for the Information Commissioner to issue fines of up to 1,000 pounds to service providers and network providers who violate the regulation.	→ The U.K. approach goes beyond what is strictly required by EU law. → Applying the EU position in the U.K. will not necessarily be sufficient for providers of electronic communications services and networks. → U.K. providers of electronic communications services and networks will need to introduce new processes in order to detect and report suspicious activity relating to unlawful direct marketing.
Article 15a (Enforcement powers) The powers of supervision and enforcement are delegated to member states to determine and therefore not specified at an EU-level.	**Clause 86 (Enforcement powers)** The current U.K. enforcement powers under the Privacy and Electronic Communications Regulations have been expanded to broadly reflect those available under the U.K. GDPR. This includes making cookie and electronic direct marketing infringements subject to increased fines of up to 20 million euros or 4% of annual worldwide turnover, whichever is higher, compared with a maximum of 500,000 pounds previously.	→ The U.K. approach goes beyond what is strictly required by EU law. → There is no direct impact on the compliance measures that need to be taken compared with the EU. → Organizations that are operating websites, mobile applications and performing direct marketing in the U.K. should be aware of the considerable increase in potential penalties for infringements.

In conclusion, the Data Protection and Digital Information Bill covers a significant number of important provisions across both the GDPR and the ePrivacy framework. However, none of the proposed changes represent a radical departure from the current law in the EU and the U.K. It is clear that with the DPDI Bill, the U.K. government has sought to simplify compliance, but not to eliminate the basic rules of U.K. data protection law. Therefore, from a compliance perspective, the essential similarities between the two regimes will not cease to exist once the DPDI Bill becomes law.