A Study On The Data Protection Laws In The Uk After Brexit

Ms. Amrita Jha

Research Scholar, Gujarat National Law University,
Gandhinagar, Gujarat, India
Email ID: amritajha93@gmail.com

Abstract

It is undeniable that the 23 June 2016 referendum opened a new chapter in the history of Europe and the United Kingdom, marred by uncertainty and, possibly, varying degrees of expectations, both on the part of the European Union and the United Kingdom. Undoubtedly, the consequences of the United Kingdom's withdrawal from the European Union are long-term and leave many questions unanswered, including the question of the right to data protection and data transfer after Brexit. This article considers how the data will continue to be protected in the UK by examining the data protection rules and regulations prevailing in the UK after its withdrawal from the EU (Brexit). This article further discusses the journey of the UK Data Protection Act from EU-GDPR to the UK-GDPR and states the status of data processing after Brexit.

Keywords**:** Data Protection, UK, Brexit, GDPR, Rights.

1. INTRODUCTION

In most countries, having control over one's personal data is a matter of fundamental right. While the European Union (EU) has adopted the omnibus approach and the United States sectoral approval, the United Kingdom (UK) is relying on a human rights-based regulatory approach for the protection of individual data. In the UK, the Human Rights Act 1998 protects the fundamental rights to privacy that domestically enforce the European Convention on Human Rights (ECHR) rights into UK law. The Human Rights Act 1998 grants fundamental rights and freedoms that also include the right to respect for private and family life, and the right to data protection is a part of that right.

Article 8 of the Convention states, "everyone has the right to respect for their private and family life, their home and

their correspondence". Despite lacking a codified Constitution, the UK has a robust set of legal frameworks that includes the Data Protection Act 2018, UK GDPR, Privacy and Electronic Communications Regulations (PECR), and common law to protect the right to privacy as a fundamental right. In addition, the Information Commission's Office (ICO) also plays a crucial role in protecting the right to data protection. The primary responsibility of the ICO is to enforce the laws and regulations related to data protection as well as guide and provide support to both businesses and individuals on these matters.

This article analyses the development of legislative proposals on data protection laws in the United Kingdom after Brexit and emphasizes the existing laws and regulations in effect.

It examines the UK legal framework to deal with the remedial perspective of privacy of individuals and businesses in the new data protection regime of the UK after the end of the Brexit transition period.

2. THE UK LEGAL SYSTEM

The United Kingdom is a parliamentary democracy and a constitutional monarchy comprised of Great Britain (England, Wales, and Scotland) and Northern Ireland. It is an island country which is located off the northwestern coast of mainland Europe. England, Scotland, Wales, and Northern Ireland, these four geographic and historical parts of the UK have their own distinct culture and history, and they are united under one political union through the Acts of Union. The UK has a constitutional monarchy, where the monarch is the head of the State but does not rule. The monarch is constitutionally obliged to follow the advice of the Government. It further has a parliamentary democracy, where the Prime Minister is the head of the Government. The UK Parliament has the ultimate law-making power. It has two Houses, the House of Lords and the House of Commons.

The House of Commons is the First Chamber of the UK Parliament, with 650 democratically elected members, known as the Members of Parliament. The primary function of the House of Commons is to represent the people of the UK in all matters, to hold the Government to account as part of the legislative process, scrutinize and approve bills, authorize taxation, scrutinize and approve the

Government's budget and planned expenditure on an annual basis, and debate the public policies of and for the Government of the United Kingdom. The House of Commons is the result of the 1215 Magna Carta of King John.

However, review of the draft government bills, investigating public policy through select committees, and making the Government accountable by asking questions to ministers in the Chamber is the primary function of the House of Lords.

Unlike other countries, the UK Constitution is not codified into a single document. Still, its core constitutional arrangements are dispersed across different leading statutes, conventions, judicial decisions, and treaties that create the institution of the State to regulate the relationships between those institutions and the relationship between the State and the individual.

In 1973, the UK joined the European Union. However, after more than forty years of participation, on 23 June 2016, a referendum was held in which the UK voters opted to leave the European Union, and as a result, Brexit happened. The word 'Brexit' describes the departure of the UK or 'British' from the EU. The withdrawal agreement was concluded between the EU and the UK in October 2019. At 11:00 PM London time on 31 January 2020, the UK left the EU, and the withdrawal agreement entered into force within UK law at the beginning of the 'transition period' that lasted on 31 December 2020. The Agreement established the terms of the UK's exit from the EU. Brexit played a vital role in the UK in assisting the fuller perception of a manifestation of the contemporary political and legal revival in the present.

3. THE UK DATA PROTECTION LAWS AND THEIR PURPOSE AND SCOPE

In any modern organization, data protection plays a significant role. Data protection can be defined as defending the personal information of individuals against any accidental or unlawful loss, destruction, alteration, unauthorized access, or disclosure and ensuring that data collection and processing is fair and does not violate privacy.

The concern for the privacy of the individual arose with the growing use of computers in the 1970s, which has resulted in many white papers, reports, and Parliamentary bills. The purpose of the data protection law is to give rights to the

people in their personal information and to restrict the ways in which organizations can use that personal information. However, the existing law at that time was insufficient to deal with the individual's concerns about their data protection. As a result, the UK created one of the world's first comprehensive legislative measures to protect people's personal information.[1] The Data Protection Act 1984 started a new regime for holding and processing online information. The 1984 Act drew on both the OECD and Council of Europe principles and the earlier work carried out by Younger and Lindop. It is based on fundamental principles for data handling, which form the code for processing personal data. It was replaced by the Data Protection Act 1998, which came into force in March 2000, aiming to broaden the scope of existing legislation and implement an EU Data Protection Directive (Directive 95/46/EC), which brought all the Member States of the European Community up to the same standard of data protection. The 1998 Act served the purpose and placed the UK at the front of global data protection standards. 2018 Act is the modernized form of the 1998 Act to make the UK law fit for the increasingly digital economy and society.

After Brexit, the EU GDPR does not apply to organizations that do domestic data processing in the UK. However, those UK organizations that process activities in both the UK and the EU or monitor EU residents' behavior are still bound by the regulatory responsibilities under both regimes, i.e., the UK regime that includes UK GDPR, UK DPA 2018 and PECR, and the EU GDPR.

"Following the Brexit transition period, the DPPEC (The Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019 combined the EU GDPR's provisions with the DPA 2018's 'applied GDPR' to form a UK data processing regime called the 'UK GDPR,' which has applied in the UK since 1 January 2021."[2] The UK GDPR can be called the retained version of the EU GDPR that came into effect on 25 May 2018. It is read with the Data Protection Act 2018, making the UK GDPR and DPA 2018 the primary legislation in the UK to regulate data privacy.

[1] Carey, Peter, *Data Protection: A Practical Guide to UK and EU Law* (5th edn, Oxford University Press 2018) 2.

[2] 'An Overview of UK Data Protection Law: The UK GDPR, DPA 2018 and EU GDPR, and the EPR and PECR' (*it governance*) <https://itgovernance.co.uk/data-protection> accessed 8 June 2023.

The preamble of the UK GDPR is comprehensive and outlines through the recitals the purpose behind the enactment of the regulation.[3] The recitals lay out in the broadest terms the necessity of enacting the provisions while recognizing the right to privacy. Similarly, the Preamble of the UK Data Protection Act 2018 states the purpose of the Act as,

"An Act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes."

Thus, the DPA 2018's goals are to regulate how personal information is processed, how the Information Commissioner handles information, how the direct marketing code of practice is implemented, and any related issues.

The UK data protection laws establish the tone and tenor of the legislation by firstly establishing the rights of individuals by empowering them to take control of their personal data and, secondly, placing well-defined responsibilities on the organizations and putting the guidelines for practices. It also provides a broad set of ancillary objectives. In addition, it elaborates on the objective by emphasizing the protection of the fundamental rights and freedom of natural persons, particularly their rights to the protection of personal data.

However, the preamble of the UK GDPR is extremely broad and includes:

- the automated or structured processing of personal data. This includes processing other than by automated means of personal data that forms part of a filing system or is intended to form part of a filing system, such as contact lists, organized paper files, address books, etc.
- the manual unstructured processing of personal data held by an FOI (Freedom of Information) public authority.

  The material scope of the UK GDPR is in the concept of 'personal data', which is extremely broad. Personal information can be any type of information that pertains to an individual. The concept of personal data

[3] 'Recitals' (*UK GDPR | Fieldfisher*) <https://ukgdpr.fieldfisher.com/recitals/> accessed 26 June 2023.

is not confined to sensitive or private information. It encompasses all types of information, either objective or subjective, provided that it relates to the data subject. Similarly, the concept of 'processing' is also broad enough to include any operation performed upon personal data by automatic means, and with regard to non-automated processing, it applies to the extent that the personal data is included in the filing system or intended to be part of the filing system.

The UK data protection law applies to the processing of personal data within the territory of the UK. It has an extraterritorial scope if the personal data of individuals located inside the UK are processed, then that company is bound by the UK data protection laws. The extraterritorial reach of the UK data protection law gives legal control to the UK on transfers of personal data outside its territory. The processing of personal data in the context of the activities of the establishment of a data controller or data processor in the UK, regardless of the place of the processing, is covered under the law.

4. THE DATA PROTECTION REGIME IN THE UK AFTER BREXIT

Worldwide internet users have reached 5.16 billion today, meaning that 64.4 percent of the world's total population is now online.[4] Out of that, 66.11 million internet users are in the United Kingdom, where internet penetration stood at 97.8 percent.[5]

The UK has enacted the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to protect personal data in the digital world. The UK GDPR forms part of the UK data protection regime along with the Data Protection Act 2018 and is based on the EU GDPR. It sets out the rules and principles for the processing of personal data. It also provides data protection rights and the data controller's and processor's obligations. The Data Protection Act 2018 is the national statute of the UK that supplements the UK GDPR. It is the cornerstone of legislation governing the treatment of personal data and received royal assent on 23 May 2018. The Act was

[4] Kemp, 'Digital 2023: Global Overview Report' (*DataReportal – Global Digital Insights*, 26 January 2023) <https://datareportal.com/reports/digital-2023-global-overview-report> accessed 24 June 2023.
[5] Simon Kemp, 'Digital 2023: The United Kingdom' (*DataReportal – Global Digital Insights*, 9 February 2023) <https://datareportal.com/reports/digital-2023-united-kingdom> accessed 22 June 2023.

implemented to keep the UK's data protection laws up-to-date and to have a well-established and well-framed data protection regime to meet the needs of the digital age in which plenty of personal data are being processed. It includes the details and the regulations to aid in the implementation and enforcement of the UK GDPR. The Data Protection Act 2018 provides matters of exemptions, enforcement authorities, and law enforcement and intelligence agencies. The Act came with an object to set new standards in the UK for the protection of personal data in compliance with the EU data protection laws to give people more control over the use of their personal data. It is structured into seven parts. Preliminary matters are mentioned under Part 1, while Part 2 supplements the UK GDPR, Part 3 of the Act is about law enforcement data processing, and Part 4 is related to personal data processing by intelligence services. The remaining parts of the Act are about the Information Commissioner, enforcement, offenses, and supplementary provisions.

The UK GDPR and the DPA 2018 protect the interests of individuals with regard to the processing of their personal data. Under DPA 2018, this protection is provided by:

- imposing the conditions that personal data should be processed lawfully, fairly, and based on the consent of the data subject;
- conferring the rights to data subjects, such as rights to obtain information about the processing of their personal data, rights to rectification of inaccurate data;
- giving the responsibility to the office holder to monitor and enforce the provisions of the Act.

The Act came as an implementation of the General Data Protection Regulation (GDPR) - the European legislation that came into force in May 2018 in the UK's national laws. However, in addition to that, it was also implemented to prepare the UK for a future outside the EU.

After the end of the transition period, the EU GDPR does not apply to the UK. The UK has already enacted the Data Protection Act 2018 to set out the rules for collecting, handling, and storing personal data. This Act came into force on 25 May 2018 by replacing the Data Protection Act 1998.

After the UK left the EU, the UK was considered a third country for data transfer to the EU. The UK ensures an adequate level of protection for personal data transferred

from the EU to the UK under the scope of the EU Regulation. Therefore, on 28 June 2021, the EU adopted an adequacy decision for the UK, ensuring the continued free flow of personal data between the two blocs for the next four years.

The Data Protection, Privacy, and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (DPPEC) has amended the UK Data Protection Act 2018 to incorporate EU GDPR requirements into UK law. It provides a new UK-specific data protection regime, i.e., UK GDPR post-Brexit. The UK GDPR is the regulation for the protection of the processing of personal data of natural persons and the free movement of such data. It forms part of the law of the UK, i.e., England, Wales, Scotland, and Northern Ireland, by virtue of section 3 of the European Union (Withdrawal) Act 2018.

The general processing of personal data is governed by Part 2 of the Data Protection Act 2018, which supplements and must be read with the UK General Data Protection Regulation (UK GDPR).[6] The UK GDPR applies to controllers and processors of personal data. Therefore, it's necessary to understand the concepts of personal data, controllers, and processors.

5. IMPORTANT TERMS: PERSONAL DATA, DATA SUBJECT, CONTROLLERS, AND PROCESSORS

The UK GDPR and DPA 2018 are applicable to **personal data** that should be related to a natural person. Under the UK data protection regime, 'personal data' is the most fundamental term and refers to 'any information or data relating to a natural person who can be identified or who is identifiable directly from the information in question or who can be indirectly identified from that information in combination with other information'.[7] Personal data also includes special categories of personal data. If an individual can be distinguished from other individuals, then that individual will be called an 'identifier' or 'identifiable.' Under the UK GDPR, a non-exhaustive list of the identifiers is provided, which includes name, identification number, location data, and an online identifier, such as IP addresses and cookies.

[6] 'Data Protection Act 2018' s 4(2)(a) & (b) <https://www.legislation.gov.uk/ukpga/2018/12/section/3> accessed 10 June 2023.
[7] ibid 3(2).

Secondly, the individual to which personal data refers is known as the '**data subject**'. Moreover, a data **controller**[8] is a person or body that determines the purposes and means of processing personal data, and data **processors** are those who are responsible for processing personal data on behalf of a controller. Controllers are the main decision-makers and exercise overall control over the purposes and means of processing personal data. If two or more controllers jointly decide the purposes and means of the same personal data, they will be called joint controllers. However, if both are processing the same data for different purposes, then they will not be called joint controllers. While the processor always works on behalf of or on the instructions of the relevant controller.

However, certain activities, such as processing covered by law enforcement directives, processing for national security purposes, and processing carried out by individuals purely for personal/household activities, are exempted from the applicability of the UK GDPR.

6. DATA PROTECTION PRINCIPLES

Key principles for processing personal data are provided under Article 5 of the UK GDPR. These principles express the spirit of the data protection regime, and failure of compliance attracts substantial fines.[9]

They are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

7. RIGHTS OF THE DATA SUBJECTS

The exhaustive rights are provided under the UK legislation for the data subjects, the people whose data is being processed. These rights include:

- Right to access: this is commonly called 'subject access request (SAR).' It gives the right to the individuals to obtain a copy of their personal data.

[8] ibid 6.

[9] See Article 83(5)(a). It states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines.

- Right to data rectification: individuals have the right to have inaccurate data rectified.
- Right to object: individuals have a right to object to processing their personal data at any time.
- Right to data erasure or right to be forgotten: the right to withdraw the consent that leads to the right to have their personal data erased is provided to the individuals; however, this right is not absolute and can only be applicable in certain circumstances.
- Right to get informed: under the UK GDPR, this is the key transparency requirement, in which individuals have the right to get privacy information, information about the collection and use of their personal data, retention periods for that personal data, and to get information with whom data has been shared.
- Right to restrict processing: individuals have the right to restrict or limit the way the organization processes that individual's personal data.
- Right to data portability: in addition to all the rights mentioned above, individuals also have
- A right to receive the personal data provided to the controller in a structured, machine-readable, and commonly used format. They can also request to transfer or move their personal data from one organization to another safely and securely without affecting its usability.

8. REGULATORY AUTHORITY

The primary regulatory authority is the Information Commissioner Office (ICO), which enforces UK GDPR and DPA 2018 in the UK and holds investigating, advisory and corrective powers. In its advisory capacity, it advises the Parliament, Government, and other institutions and bodies on legislation-related matters to ensure data subject rights and personal data processing. In addition, it is also responsible for presenting an annual report on the infringements that happened and the measures taken for that. Handling the complaints lodged by the data subjects and maintaining the public register of certification mechanism, data protection seals, and marks are also the functions of the ICO. ICO is also responsible for promoting awareness among the public about risks, safeguards, rules, and rights in relation to processing. Along with that, it also spreads awareness among controllers and processors on their obligations. It also plays an advisory role and can

prepare a code of practice to provide practical guidelines for sharing personal data according to data protection legislation's requirements.

9. PENALTIES FOR NON-COMPLIANCE

Under the UK GDPR and DPA 2018, administrative fines can be imposed on organizations or persons for infringements and non-compliance notices. A number of factors, including negligence, the controller's or processor's responsibilities, the categories of personal data affected by the violation, the action taken by the controller or processor to lessen the harm, adherence to the codes of conduct or certification procedures, and the controller's or processor's prior violations, if any, are taken into account when determining the administrative fines and their amount.

Generally, when the rules provided under UK GDPR and DPA 2018 are not followed on matters related to the basic principles of processing, including consent, data subject rights, cross-border transfer of data, or non-compliance with an order of ICO, the penalties are imposed.

10. CONCLUSION

To conclude, the UK has proved itself to be a torchbearer in the field of legislative functions worldwide. It is one of those countries that implemented laws for protecting personal data years ago. It sets out adequate standards to protect individual data by giving them more control over the use of their data and providing them the unique right of portability or data erasure. An utmost priority in regulating and safeguarding the personal data of individuals is given under the UK data protection regime. At the same time, it also ensures tailored exemptions for e-commerce entities and organizations for research and modern innovation.

It also provides a bespoken regime for law enforcement purposes, in which police, prosecutors, intelligence services, and other criminal justice agencies will be exempted from processing personal data while ensuring that the laws have adequate safeguards and modernized international standards.

Therefore, it will not be exaggerated to conclude that the UK Data Protection legal framework is the most advanced and certainly the most comprehensive code ever to be enacted in any country in the sphere of data protection.