UK Data (Use and Access) Act, 2025 - Echoing India's DPDP Law Free

Jul 01, 2025

K. Vaitheeswaran
Advocate

Srividya. S.U
Advocate

The UK GDPR and the Data Protection Act, 2018 are seen as the primary sources of inspiration for India's Digital Personal Data Protection Act, 2023. However, with the UK's Data (Use and Access) Act, 2025 (DUAA Act, 2025) receiving Royal Assent on 19.06.2025 an intriguing reversal of roles seems to have taken place. With the generous usage of undefined yet powerful terms like 'national security', 'public interest', 'archiving', 'research' etc, UK Lawmakers sure seem to have drawn inspiration from exactly those parts of Digital Personal Data Protection Act, 2023 which were criticised for their potential to be misused as tools for processing of personal data by the State without specific consent of the data principal.

The wide range of changes made to the UK GDPR and the Data Protection Act, 2018 are concealed within the Preamble of the DUAA Act, 2025 Act with an unassuming description such as "to make provisions for the regulation of the processing of information relating to identified or identifiable living individuals".

However, a thorough analysis of the amendments made to both the UK GDPR and the Data Protection Act, 2018 vide Part 5 of the DUAA Act, 2025 will echo the concerns raised in India on the role of the State.

Legitimate Interests

In India, processing for the *performance of functions under any law by the State or its instrumentalities or in the interest of sovereignty and integrity of India or security of the State, for fulfilling obligations of disclosure under any law to the state or its instrumentalities, for providing assistance to any individual during any breakdown of public order* are recognized as legitimate purposes for processing of personal data vide Sections 7(c), (d) and (h) of the DPDP Act, 2023. However, none of the exempted purposes are defined in the Act.

Similarly, Section 70 and Schedule 4 of The DUAA Act, 2025 have introduced a list of legitimate interests by inserting Annex I to the UK GDPR whereby processing of personal data for *the performance of a task of the controller carried out in public interest or a task carried out in the exercise of official authority vested in the controller, archiving in public interest, public security, emergencies, crime, protecting vital interests of data subjects and safeguarding vulnerable individuals* are now recognized as legitimate interests that would constitute lawful processing under Article 6 of the UK GDPR. This in effect means that no specific consent of the data principal would be required if the data is processed for the said legitimate interests.

Further, the Secretary of State has been granted powers to alter the list of legitimate interests as required by making regulations. *This is akin to the routine Indian lawmaking style of expansion through notifications.*

Compatible Purposes

Amendments have now been carried out by way of insertion of Article 8A to the UK GDPR vide Section 71 of the DUAA Act, 2025 to recognize processing of personal data without specific consent, in certain scenarios, as *"processing in a manner compatible with the original purpose."* This, in effect, means that, there is no need to obtain fresh consent from the data principal if the processing is for these newly recognized purposes and safeguards such processing. Processing for scientific/historical research, archiving in public interest and for statistical purposes are now recognized as processing compatible with the original purpose.

Schedule 5 of the DUAA Act, 2025 inserts Annex 2 to the UK GDPR which lists out more scenarios where processing without specific consent of the data principal will be legal by virtue of it being considered as processing compatible with the original purpose. The scenarios listed in Annex 2 are *disclosure for archiving in public interest, public security, emergencies, crime, protection of vital interests of data subjects and others, safeguarding vulnerable individuals, taxation and legal obligations.*

Interestingly, no meaning has been provided for the phrase 'archiving in public interest' and the term 'public interest' has also not been defined. 'Scientific research purposes' has been defined as *processing for the purposes of any research that can reasonably be described as scientific.* The provision also clarifies that such an exemption would extend to public or privately funded research and also to commercial and non-commercial research. The scope is clearly wide.

Similar provisions can be traced back to Section 17(2)(b) of the DPDP Act, 2023, and Rule 15 of the draft DPDP Rules, 2025 which exempt the processing of personal data for research, archiving or statistical purposes, from the application of the provisions of the Act and once again, such exempted purposes are not defined and are left to the imagination.

National Security and Law Enforcement Processing

Section 17(2)(a) of the DPDP Act, 2023 exempts the "instrumentalities of the State" from the provisions of the Act when they process personal data in the *"interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these".*

Right to be forgotten is also curtailed in matters where personal data is processed by the State or its instrumentalities as Section 17(4) exempts them from the requirement to erase personal data under Sections 8(7) & 12(3) of the DPDP Act, 2023 on a request from the Data Principal.

Section 11(2) of the DPDP Act, 2023 curtails the right of the data principal to seek information about the processing of their personal data in cases where it is shared pursuant to a written request for the *"purposes of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences".*

Section 17(1)(c) of the DPDP Act, 2023 exempts the application of the provisions related to the obligations and rights of the data fiduciary and the data principal respectively, when personal data is processed *"in the interest of prevention, detection, investigation or prosecution of any offence or any contravention of any law."*

Similarly, Section 88 of the DUAA Act, 2025 inserts Section 78A to the Data Protection Act, 2018 which grants wide exemptions from the provisions safeguarding the interests of the data principal when the processing is for law enforcement purposes for safeguarding National Security. The power to grant such exemption is left to the judgment of Ministers of Crown who are empowered to grant certificates stating that such exemption from the application of the provisions was necessary in the interest of National security and further, such a certificate is considered as conclusive proof of the need for such an exemption.

Section 89 of the DUAA Act, 2025 inserts Section 82A to the Data Protection Act, 2018 thereby empowering the Secretary of State to issue a notice, designating a competent public authority to jointly process personal data for safeguarding national security with intelligence services.

Section 85 of the DUAA Act, 2025 makes amendments pertaining to transfer of personal data to third countries and international organizations for law enforcement processing and empowers the Secretary of State to make regulations and approve such transfers if the data protection test is met. The data protection test primarily attempts to ascertain if the data protection standards in the country or international organization of transfer 'is not materially lower' than the standard of protection provided for data principals in the UK.

Section 16 of the DPDP Act, 2023 provides that the Central Government may by notification, restrict the transfer of personal data by a Data Fiduciary for processing to a territory outside India. This is indicative of the fact that a robust mechanism to govern transfers of personal data for processing outside India does not exist as on date. Rule 14 of the draft DPDP Rules, 2025 also merely provides that the transfers of personal data outside India to a *foreign State, or to any person or entity under the control of or any agency of such a State* shall be compliant with the general or specific orders of the Central Government. Therefore, the Indian law may follow the amended UK law and may permit such transfers in scenarios where the Government is satisfied that the data protection standards in the other country 'is not materially lower'.

Section 40 of the DPDP Act, 2023 bestows the Central Government with wide powers to make rules for carrying out the purposes of the Act and *any other matter which is to be or may be prescribed or in respect of which provision is to be, or may be, made by rules.*

Similarly, the DUAA Act, 2025 contains many such provisions that bestow wide discretionary powers on the Secretary of State or other Ministers to make regulations, being classic examples of Henry VIII Clauses *(delegated legislative powers that allow the Government to amend primary legislation by way of secondary legislation).*

Transparency

Control to the data principal on the processing of their personal data, the right to seek information on such processing and prevention of any processing prejudicial to their interests are sacred elements of global data protection laws with transparency as one of the primary attributes.

Section 77 of the DUAA Act, 2025 makes certain amendments to Article 13 of the UK GDPR to the extent that information about processing of personal data need not be given to the data principal if the processing if the additional processing is solely for the purposes of scientific or historical research, archiving in public interest or statistical purposes. Further, the Section goes on to state that such information on additional processing of personal data need not be shared with the data principal if 'providing such information would involve a disproportionate effort' and 'disproportionate effort' is also given a vague description.

Section 78 of the DUAA Act, 2025 amends Article 15 of the UK GDPR and Sections 45 and 94 of the Data protection Act, 2018 to provide that the data subject is only entitled to such confirmation, personal data and other information as the controller is able to provide based on a reasonable and proportionate search. However, the amendments don't specify as to what constitutes a *'reasonable and proportionate search'*. Notably, Section 45 and 94 fall under Part 3 and 4 of the Data Protection Act, 2018 which contain provisions relating to law enforcement processing and intelligence services processing respectively.

Sections 11(2) and 17(1)(c) of the DPDP Act, 2023 are similar provisions in India where the rights and obligations of the data principal and the data

fiduciary respectively are suspended when processing of personal data is done for law enforcement purposes or by the State or its instrumentalities.

Such exemptions from providing information about the processing of personal data to the very individual whom the data pertains to strikes at the very cornerstone of data protection laws which attempt to achieve a balance between the rights of data principals and the need to process personal data while preserving the rights of the data principal. The dilution of the rights of the data principal can be a matter of concern.

Takeaways

The specific amendments discussed above are not the only areas of concern considering the wide powers given to office bearers of the State to make secondary legislation in the areas pointed out above. With various provisions taking effect in a staggered manner, a true assessment of the impact of these changes on privacy and rights of data principals can only be made with passage of time. The requirement to submit an annual report on regulatory action, safeguards and restrictions placed on automated decision making and changes in relation to digital verification services are some positive takeaways from the DUAA Act, 2025.

India has enacted the DPDP Act, 2023 and the effective date is yet to be notified. Draft rules have been placed in the public domain and Ministry of Electronics and Information Technology (MeitY) has held extensive rounds of meetings with stakeholders on the scope and ambit of the Rules. It is interesting to note that the UK GDPR is getting modified by echoing some elements from the Indian Law. As the years roll on this branch of law will play a very pivotal role for all concerned.