Distinction between UK Data Protection Act 1998 and EU's GDPR

The enterprise business data is a heart of any enterprise to run their operational business activities. The essence of safeguarding personal data is gaining momentum compare to previous decades due to stringent penalty and guidelines from the regulatory bodies across the globe. This article compare the distinction between UK Data Protection Act 1998 and newly proposed European Union's GDPR (General Data Protection Regulation) on key attributes.

#	Attribute	UK Data Protection Act 1998	EU's GDPR
1	Privacy law implementation	• Year 1994 - UK introduced its first Data Protection Act • Year 1998 - UK Data Protection Act	• The European Parliament and the Council of the European Union introduced the new regulation GDPR on 27th April 2016 • All the enterprise both Government and Private Sectors must comply with GDPR by May 2018
2	Principles	Data Protection Act is based on 8 data protection principles	GDPR is developed using 6 data privacy principles
3	Data Controller	• A person or a group determines the purposes for which any personal data are processed • It is an organization or an individual who act on behalf of an organization • Ensure that the data are processed in compliance with Act.	Accountable for failures of any data processor and equally liable for any breaches.
4	Role of ICO and DPO	<u>The Information Commissioner's Office (ICO)</u> • Promote good practice of personal data handling • Provide guidance and advise on data protection • Maintaining list of organization in the form of register to get notification about information processing activities • Resolve any disputes that related to an enterprise compliance with data protection act on data processing • Enforce compliance with Act • Prosecute the offences committed under the act	<u>The Data Protection Officer (DPO)</u> • The DPO may provide advice to data controller on data protection impact assessment • The DPO shall be legal expert in data protection • Monitor the compliance with Regulations • Point of contact with Supervisory authority
5	Consent from the individual	An enterprise • Need to get consent from an individual before disclosing information to any third parties • Need to get prior consent from an individual to use or disclose personal data for any additional purpose other than initial consent.	An individual need to provide consent for every data processing activities
6	Right of an individual	• Only the enterprise can update customer's personal data upon data received from an individual or from any authority third party source. • It is possible that an enterprise may maintain an individual's past data until he / she provides their latest data such as address with relevant convincing documents to an enterprise • The individual can opt not to do business relationship with an enterprise when their data to be disclosed to third parties and he / she is not clearly aware of purpose of such a disclosure • Has right to get copy of their data	• Need to provide consent for every data processing activities • Must manually tick the box as consent • Can request the data to be transmitted within EU for another data controller • has direct access to his/her data in the enterprise such as web based portal application • He or She can erase the data under some scenarios

		• Right to object to processing that may cause damage • Right to rectify the incorrect data , blocked and erased • Right to claim compensation for damage caused by data breaches as specified in the data protection act	
7	Children's personal data	Parental consent is required for children under the age 12. When the risk level is high, the parental consent is required for the children aged above 12.	• Children under age 16 cannot provide their consent to data collection or data processing. • Parental or authorized consent is required for the children under age 16 • Whenever a direct counselling services offered to child about data privacy, the consent from parents are not necessary.
8	Notification	• The organization must notify the ICO (The Information Commissioner's Office) on details of data being processed, the details includes data recipients ; how is the data being processed in a generic manner to meet statutory requirements • The enterprise need to communicate the data breach to appropriate people and organization.	• When the personal data breach happened, the data controller must notify the supervisory authority within 72 hours of the data breach has been noticed • If the data breach notification is not done within 72 hours, reasons for the delayed communication must also be notified • The data controller should communicate to the natural person about personal data breach without undue delay • When the data breach has happened, if the risk to the natural person is high, the data controller must communicate to the natural person about data breaches without any delay • The data controller communicate to the customer about recertification of the data or eraser of personal data or any restriction of data processing.
9	Exemptions from notification	Organization process • Data for their own business activities • Personal data for the staff administration • Data for Non-Profit Organization • When the computer is not used to process the data • Personal data for purposes relating to criminal justice and taxation	• As per GDPR article 89 (1), the personal data that is used for scientific and research purpose can be retained for longer time provided appropriate technical controls are in place • Personal data are processed for Archiving purpose in the interest of public interest. • Personal data are processed for historical and statistical purpose
10	Penalty	• The ICO has statutory power to impose financial penalty on an organization. The monetary penalty cannot be exceed £ 500,000 • The financial penalties apply only if the breach is deliberate or organization is failed to mitigate the risk despite aware of this • The data controller or a person to whom a monetary notice has been served may appeal against the penalty specified in the notice.	• The penalties are proportioned to the compliance failure • Higher penalties - Up to 20 000 000 EUR or 4% of total worldwide annual turnover of previous financial year, whichever is higher • Lower Penalties - Up to 10 000 000 EUR 4% of total worldwide annual turnover of previous financial year, whichever is higher • The penalties are depends on defined article provisions by the GDPR.

11	Pseudonymisation and Encryption of personal data	The data protection act does not require an enterprise to encrypt personal data. However, it is an enterprise's responsibility to deploy appropriate controls to safeguard the personal data.	• Implement appropriate technical and organization protection measures to protect the personal data such as encryption to prevent unauthorized access to the data • Using Pseudonymisation to personal data can reduce the risk to an individual. The additional information about an individual will be stored separately. The part of the personal data will be replaced by unique identifier. When combine real additional information (that was replaced with unique identifier) with part of the data may reveal original identity of an individual.
12	Cross border data transfer	Need to consent from an individual before transmitting data to other countries. Transfer the data to other countries only if they have adequate data protection laws to protect individual data.	Need to consent from an individual before transmitting data to other countries. Transfer the data to other countries only if they have adequate data protection laws to protect individual data.