GDPR, DPA, PECR AND ePRIVACY EXPLAINED

	1998 Data Protection Act	2016 General Data Protection Regulation	2003 Privacy and Electronic Communications Regulation	2017 ePrivacy Regulation
How does it define personal data?	Information that relates to an identifiable individual and is processed, wholly or partly, by automatic means or by non-automated processing within a filing system	Extends the range of information covered by the DPA to include genetic and biometric data, as well as online identifiers such as IP addresses	Same as DPA	Same as GDPR
How does it benefit individuals?	Individuals benefit from controls imposed on how their personal data is used by data controllers. Controllers must adhere to the 'data protection principles' which are detailed in the DPA. For a list of the principles, visit: *ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/*	Individuals will be able to control how their data is used, know where it is stored and have a right to transfer or, in some circumstances, erase it. In instances of misuse, individuals will have increased rights to legal recourse alongside existing rights to claim compensation	Individuals are given specific privacy rights in relation to electronic communications, including marketing communications, and in relation to the use of cookies	Individuals will enjoy sufficient protection against unauthorised access or alteration to electronic communications data and confidential and safe transmission
How does it affect companies?	Companies may only process data in accordance with the 'data protection principles', and must allow individuals to exercise certain rights over their personal data	Companies that process personal data must have robust policies and procedures in place to comply, and demonstrate compliance, with the GDPR from 25 May 2018. Processing must only be performed with the appropriate consent or in reliance on another legal basis. Companies must have policies in place to allow data subjects to exercise their rights under GDPR. Both data controllers and data processors are subject to the GDPR, though the obligations on processors are more limited	Companies must ensure they have the necessary consents to electronic direct marketing. The requirements are different depending on the form of electronic communication. A company must also obtain consent for any cookies 'dropped'	Companies will need to review their consent mechanisms and any reliance on cookies for marketing, to ensure that the business can continue to communicate with consumers in the way that it wants to. The requirements are stricter than in the PECR
Penalties for non-compliance	Maximum fine of £500,000	Maximum fine of 4% of annual global turnover or €20m, whichever is higher	Maximum fine of £500,000	Maximum fine of 4% of annual global turnover or €20m, whichever is higher
Territorial scope	DPA applies to data controllers established in the UK, which are processing data in the context of that establishment; or where the controller is established outside the UK/EEA, but is processing data using equipment in the UK otherwise than for transit	GDPR will apply to the processing of personal data by businesses established within the EEA, and to controllers or processors established outside the EEA that are conducting processing activities related to the offering of goods or services to individuals within the EEA, or monitoring the behaviour of individuals within the EEA	PECR does not have extraterritorial effect, so organisations outside the EEA are not subject to its obligations	ePrivacy will apply to entities anywhere in the world that provide electronic communications services to, or gather information related to the terminal equipment of, end users within the EEA

Source: RPC