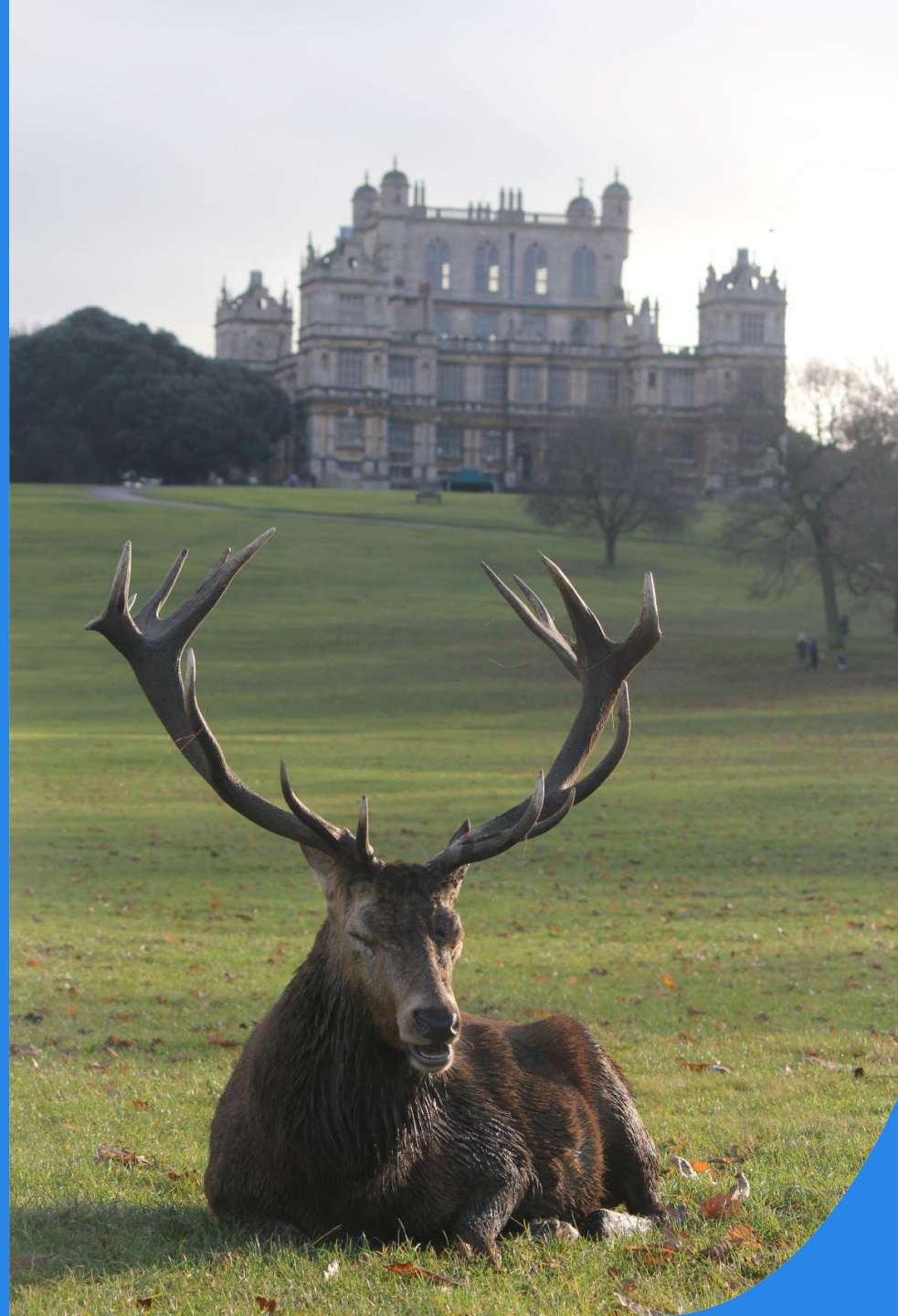
u3a learn, laugh, live

Wollaton

GDPR

General Data Protection Regulations



u3a

This information is general guidance and does not constitute legal advice

u3a

What is the GDPR?

The General Data Protection Regulation (GDPR), which came into effect on 25th May 2018, provides a legal framework for keeping everyone's personal data safe by requiring companies to have robust processes in place for handling and storing personal information. It's also designed to protect us as individuals from being contacted by organisations without our express permission.

Why Does it Matter?

The GDPR is bigger than its predecessor, the Data Protection Act 1998 (DPA 1998), and ushered in a wave of new rules which are significantly different in certain areas, such as:

- A wider definition of 'personal data' which covers more information than ever before;

- Data processors (i.e. firms that process personal data on behalf of another business, such as an outsourced payroll service) will be required to comply with the GDPR, whereas they weren't required to comply with the DPA 1998;

- When obtaining 'consent' from individuals, it must now be explicit and specific – it's all about 'opting in' (and knowing exactly what we're signing up for) rather than 'opting out'. The old rules placed the onus on the individual to ask to be removed from a mailing list. In future, businesses must ask for consent from the very start;

- A duty to report data breaches to the Information Commissioner within very strict timeframes;

- A new 'right to be forgotten';

- The statutory need for certain businesses to appoint data protection officers, responsible for overseeing the new requirements for record-keeping and data impact assessments;

- An easier process for individuals to claim compensation from a non-compliant business; and tougher penalties for non-compliance.

What are the 6 principles of GDPR?

The 6 core principles of the GDPR are:

• Fairness, Lawfulness and Transparency. You much be *fair*, *honest*, and *transparent* with individuals whose data you are processing.

• Purpose Limitation. You must be clear about your purpose(s) for processing personal data.

• Data Minimisation. You should only process the information that you need to make a decision.

• Accurate and relevant. keep personal data accurate and up to date.

• Storage Limitation. You should only keep the individual's data for as long as is necessary.

• Integrity & Confidentiality. You must keep personal data safe and secure.

Accountability. Whilst not a core principle, it does underpin the above principles. You must be responsible and adhere to the rules of GDPR. (Under the original Data Protection Act (DPA) 1998, there were 8 principles. 6 of these were like the current GDPR principles above. Originally, they were fairness and lawfulness, purposes, adequacy, accuracy, retention, rights, and security).

What is classed as 'personal data'?

Any information relating to an individual that directly or indirectly allows them to be identified or distinguished from other individuals.

How long can I keep personal data for?

Only for as long as you are actively and legitimately using it. As soon as you no longer need the data, you should destroy it. Exceptions are reasons that relate to archiving purposes in the public interest, scientific or historical research, or statistical purposes.

Can users opt out of GDPR?

No. Any business or organisation that processes personal data must comply.

What are the 6 principles of GDPR?

The 6 core principles of the GDPR are:

• Fairness, Lawfulness and Transparency. You much be *fair*, *honest*, and *transparent* with individuals whose data you are processing.

• Purpose Limitation. You must be clear about your purpose(s) for processing personal data.

• Data Minimisation. You should only process the information that you need to make a decision.

• Accurate and relevant. keep personal data accurate and up to date.

• Storage Limitation. You should only keep the individual's data for as long as is necessary.

• Integrity & Confidentiality. You must keep personal data safe and secure.

Accountability. Whilst not a core principle, it does underpin the above principles. You must be responsible and adhere to the rules of GDPR. (Under the original Data Protection Act (DPA) 1998, there were 8 principles. 6 of these were like the current GDPR principles above. Originally, they were fairness and lawfulness, purposes, adequacy, accuracy, retention, rights, and security).

Four Things to Check Now

Here are five things that you need to address, if you haven't already.

- **Information held:** do you know what personal data you currently hold, where it came from and what it is used for? If not, carrying out an information audit will help identify areas for reform;

- **Privacy notices:** check your current privacy notices (the statement that describes what you use data for), do they meet GDPR requirements? Remember they should be kept under continuous review and updated when something changes;

- **Rights:** ensure that your procedures cover all the rights of an individual, including how data would be provided in response to a request or how you might action a request for erasure;

- **Gathering consent:** does how you gather and record consent comply with the GDPR?

u3a learn, laugh, live

Further information about u3a Wollaton and its policies can be found at the following website (links below)

Wollaton U3A: Home (u3asites.org.uk)

Wollaton U3A: Documents (u3asites.org.uk)