New General Data Protection Regulations (GDPR)

Main changes coming into effect in the UK on 25 May 2018

At a Glance

Please see a quick chart together and a 12-step guidance plan from the Information Commissioners Office (ICO) here: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Background

The European Union have introduced the GDPR to update and harmonise data protection practices across the EU. It will apply to all European Economic Area countries (EEA) and also to any individual or organisations trading with them. As it comes into force in the EEA on 25 May 2018 (i.e. before the UK leaves the EU), UK individuals and organisations must ensure compliance with the new regime by then.

The ICO and the government have confirmed that they expect UK individuals and organisations to adhere to the GDPR, as post-Brexit the UK's data protection legislation (currently the Data Protection Act 1998 (DPA)) must meet the GDPR standard.

Why the change?

The GDPR aims to update data protection to meet the new challenges of the 21st century. It increases protection for consumers and places increased obligations on individuals and organisations to both ensure and evidence that they handle personal data correctly and securely.

What is the same?

- The definitions of Data "Controller" and "Processor"
- The ICO will remain as the UK's regulator
- The eight current Data Protection principles will still apply
- The rules regarding International data transfers will still apply i.e. outside the EU

What has changed?

- Data Controllers have some new obligations.
- "Accountability principle" – when necessary, you must be able to show how you comply with the data protection rules e.g. document what you have done and why.
- Data Processors must now maintain records and are directly liable if responsible for a breach
- Privacy Impact Assessments - must be carried out to assess the risk to individuals' rights, e.g. when using new systems or technology.
- There are higher standards for obtaining and proving 'consent'.
- Enhanced rights for individuals - including the right to be informed, object and (where applicable) 'be forgotten' as well as rights regarding access, rectification, erasure, restrictions on processing, data portability and automated decision making of their personal data.
- Appointment of a Data Protection Officer (DPO) – however, not mandatory for all organisations e.g. Scout Groups, Districts or Counties/Areas/Regions, however, an appropriately senior individual must be responsible for GDPR compliance.
- The duty to report a breach quickly will apply to all and failure to report will result in a fine.

- Increase in maximum fines (up to 4% of global annual turnover).

Further updates/guidance
The Scout Association is monitoring further advice from the ICO as and when it arises and will provide further updates to members over the coming months. However, for present purpose, it is important to note that:

1. Each Scout Unit (Group, District and County/Area/Region) will still be a Data Controller and, therefore, overall responsibility for compliance with data protection will lie with the Executive Committees of each Unit who, as the Managing/Charity Trustees, are jointly responsible for all the affairs of the Unit. However, Executive Committees should consider designating someone to take responsibility for compliance.

2. As smaller 'not-for-profit' organisations, Scout Units still do not have to formally register with the ICO as data Controllers provided they do not hold personal data about anyone other than members or potential beneficiaries. However, they will still be subject to the rules of the GDPR.

3. As a larger organisation, The Scout Association Headquarters is already (and will continue to be) registered as a Data Controller with the ICO.

4. The current 40 day deadline for complying with a Subject Access Request "SAR" (i.e. sending someone all their personal data held by a Scout Group, a District or a County/Area/Region) is being reduced to 30 days.

Please note: The above is intended as general advice only and, where needed, you should check the ICO website for more detailed guidance/advice https://ico.org.uk/