Privacy Protection Policy for Scrutineers

What does this mean to you, as a scrutineer/volunteer?

The General Data Protection Regulations (GDPR) sets out requirements for how organisations need to handle personal data from 25 May 2018. As a Scrutineer, SoBRA regularly shares with you the personal details of applicants seeking accreditation. SoBRA has updated its Privacy Policy, a copy of which can be found on our website. SoBRA must ensure that its scrutineers and volunteers are aware of this policy and that they understand their individual responsibilities.

Data storage and Use

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the SoBRA data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- If you download an applicant's documentation sent to you as a Scrutineer, please ensure that you delete the documents from your computer after you no longer require them. Alternatively, view the documents on your computer and avoid downloading at all, although it is appreciated this is sometimes not practical.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Paper and printouts are not to be left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Personal data must be encrypted before being transferred electronically.
- SoBRA representatives should seek to avoid saving copies of personal data to their own computers.
- Always access and update the central copy of any data.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.

- Data should not be saved directly to laptops or other mobile devices like tablets or smart phones although it is appreciated this is sometimes not practical.

If you believe you may have accidentally lost or had stolen a device or paperwork containing personal data, please report immediately to SoBRA. We have 72 hours to report certain incidents to the Information Commissioners Officer (ICO). If we fail in this measure, we face potential fines and/or other sanctions. It is important that, no matter how small you believe the breach may be, or if you are simply unsure, you report it as soon as possible. Just in case. It is then for the SoBRA Committee to decide whether the incident should be notified to the ICO.