SoBRA
The Society of Brownfield Risk Assessment

Data Protection Policy

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations need to handle personal data from 25 May 2018.

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. The focus of the GDPR is upon ensuring fairness, transparency, accuracy, security, minimisation and respect for the rights of the individual whose data we want to process.

Key Details

Policy Prepared by:	Dr Alexander Lee, SoBRA Chair
Approved by Executive committee on:	17 May 2018
Policy became operational on:	25 May 2018
Next review date:	Annually at year start of October

Note: SoBRA does not have to register with the Information Commissioners Office (ICO) as we are a not-for-profit organisation. A specific exemption applies to bodies or associations that are not established or conducted for profit. However, the exemption applies only if:

- SoBRA are only processing data for the purposes of establishing or maintaining membership or support for a body or association not established or conducted for profit, or providing or administering activities for individuals who are members of the body or association or have regular contact with it;
- SoBRA only hold information about individuals whose data it needs to process for this exemption purpose; and
- the personal data SoBRA process is restricted to personal information that is necessary for this exemption purpose.

Introduction

At SoBRA, we are committed to protecting and respecting your privacy.

This Policy explains when and why we collect personal information about people who visit our website, how we use it, the conditions under which we may disclose it to others and how we keep it secure. We may change this Policy from time to time so please check this page occasionally to ensure that you're happy with any changes. By using our website, you're agreeing to be bound by this Policy. Any questions regarding this Policy and our privacy practices should be sent by email to info@sobra.org.uk.

SoBRA
The Society of Brownfield Risk Assessment

Who are we?

The Society of Brownfield Risk Assessment (SoBRA) has been established to support the growing number of professionals working in land contamination risk assessment. It is a learned society for individuals, with membership drawn from the private, public, voluntary and academic sectors. Its goals are to improve technical knowledge in risk-based decision-making related to land contamination applications and to enhance the professional status and profile of practitioners. SoBRA is a not for profit society.

Responsibilities

Everyone who works for or volunteers with SoBRA has some responsibility for ensuring personal data is collected, stored and handled appropriately.

Each member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, the following people have key areas of responsibility:

- The Executive Committee is ultimately responsible for ensuring that SoBRA meets its legal obligations.
- The Data protection officer, [to be named annually], is responsible for:
    - Keeping the Executive Committee updated about its data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for new committee members.
    - Handling data protection questions from the Executive Committee and members.
    - Dealing with requests from individuals to see the data that SoBRA holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle members information (e.g. our secure web provider).
- The Web manager/IT manager, [to be named annually], is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
- The marketing manager, [to be named annually], is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Where necessary, working with other Executive Committee members or SoBRA members to ensure marketing initiatives abide by data protection principles.

How do we collect information from you?

We obtain information about you when you register as a member of the society through our membership payment platform or if you register to receive one of our newsletters or attend one of our

webinars. Furthermore, we receive information from applicants when they seek to apply for accreditation with the Society. We collect information in the following ways: -

- Email
- Online form
- Paper forms
- Excel and Word documents
- PDF Documents (Scans)

What type of information is collected from you?

SoBRA will never collect any unnecessary personal data from you and will not process your information in any way, other than as specified in this notice. We will only use people's data in ways they would reasonably expect and which have a minimal privacy impact. The personal data that we collect from you includes:

- Name
- Date of Birth
- Home Address
- Business/ Institute Address
- Personal Email
- Business Email
- Home Telephone Number
- Mobile Telephone Number
- Paypal, Bank or card details (to process payments for membership, conference/workshop attendance, for example)
- Signature (on paper forms such as accreditation application forms)
- Status/ Qualifications/ Academic history and CV for those applying for accreditation

How is your information used?

The purposes and reasons for processing your personal data are detailed below:

- process a payment that you have made;
- process requests that you have submitted;
- carrying out our obligations arising from any contracts entered into by you and us;
- when seeking your views or comments on the services we provide;
- when notifying you of changes to our initiatives;
- send you communications which you have requested or that may be of interest to you. These may include information about webinars, conferences, news, other initiatives; and
- processing a membership, accreditation and /or sub-group application.

This processing is necessary for membership contracts and for members legitimate interests.

Note. We will review our retention periods for personal information on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. We will hold your personal information on our systems only for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

Who has access to your information?

Only SoBRA approved committee members and selected representatives on a needs only basis have access to your information. We will not sell or rent your information to third parties. We will not share your information with third parties for marketing purposes. Scrutineers of the accreditation applications process access specific applicant's data, but have access only by a secure web page and are also bound by the terms and contents of this policy.

Third Party Service Providers working on our behalf:

We may pass your information to our third-party service providers for the purposes of completing tasks and providing services to you on our behalf (for example to process payments and send you mailings). However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure and not to use it for their own direct marketing purposes.

Please be reassured that we will not release your information to third parties beyond SoBRA for them to use for their own direct marketing purposes, unless you have requested us to do so, or we are required to do so by law, for example, by a court order or for the purposes of prevention of fraud or other crime.

Third Party Product Providers we work in association with:

When you are using our secure online payment pages, your payment is processed by a third-party payment processor, who specialises in the secure online capture and processing of credit/ debit card transactions. If you have any questions regarding secure transactions, please contact us. We do not know or save your credit card details.

We may transfer your personal information if we're under a duty to disclose or share your personal data in order to comply with any legal obligation or to enforce or apply our terms of use or to protect the rights, property or safety of our members. However, we will take steps with the aim of ensuring that your privacy rights continue to be protected.

Your choices (consent)

You have a choice about whether or not you wish to receive information from us. If you do not want to receive communications from us about the work we do and our webinars, conferences or other services, then you can select your choices by ticking the relevant boxes situated on the annual renewals form on which we collect your information.

Existing members (May 2018) have been offered a positive opt-in service to continue to receive information from us. Consent is not a precondition of service. Furthermore our obligations don't end when we first get consent. SoBRA will continue to review consent as part of our ongoing relationship with members and refresh it if anything changes.

How you can access and update your information

The accuracy of your information is important to us. We're working on ways to make it easier for you to review and correct the information that we hold about you. You can check and change your

information at any time by checking your account details when logging into your SoBRA account or emailing info@sobra.org.uk (Right to rectification and data quality).

All individuals who are the subject of personal data held by SoBRA are entitled to:

- Ask what information SoBRA holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how SoBRA is meeting its data protection obligations.
- If an individual contacts SoBRA requesting this information, this is called a 'subject access request'.

Subject access requests from individuals should be made by email, addressed to the data controller at info@sobra.org.uk. Individuals will be charged £10 per subject access request. SoBRA must provide information without delay and at least within one calendar month of receiving it. SoBRA can extend this by a further two months for complex or numerous requests (in which case we must inform the individual and give an explanation).

The data controller will always seek to verify using "reasonable means" the identity of anyone making a subject access request before handing over any information.

Right to erasure including retention and disposal

Individuals have the right to be forgotten and can request the erasure of personal data when:

- it is no longer necessary for the purpose SoBRA originally collected/ processed it for;
- the individual withdraws consent;
- SoBRA are relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest for SoBRA to continue this processing; and
- it was unlawfully processed (i.e. otherwise in breach of the GDPR);

Individuals can make a request for erasure verbally or in writing. SoBRA will seek to verify the identity of the person making the request, using "reasonable means". SoBRA should respond to a request without delay and at least within one month of receipt.

A written retention policy or schedule will be used to remind SoBRA when to dispose of various categories of data, and help SoBRA plan for its secure disposal. SoBRA will designate responsibility for retention and disposal to an appropriate person.

Security precautions in place to protect the loss, misuse or alteration of your information

We currently employ the following security precautions to protect any personal data/information held by our organisation:

- All our data/information on members is held in a secure server with up to date firewalls, encryptions and strong password protection;
- All members are required to use a strong password protection for their individual account;

- The back end of the website has restricted access to the website designer, and limited access to the website co-ordinator and the Accreditation Administrator;
- PayPal handle all our members bank details and these details are not kept anywhere else. PayPal has extensive security measures in place and the only person that will access Paypal is the SoBRA Treasurer and Chair.
- Any data/ information held in Dropbox is only accessible to the current Executive Committee Members. Dropbox security includes two stage verification, strong passwords and 256-bit Advanced Encryption Standard

Profiling

We do not analyse or plan to analyse your personal information to create a profile of your interests and preferences.

Use of 'cookies'

The SoBRA website does not use cookies other than Google Analytics.

Links to other websites

Our website may contain links to other websites run by other organisations. This policy applies only to our website, so we encourage you to read the policy statements on the other websites you visit. We cannot be responsible for the policies and practices of other sites even if you access them using links from our website.

In addition, if you linked to our website from a third-party site, we cannot be responsible for the policies and practices of the owners and operators of that third-party site and recommend that you check the policy of that third-party site.

The processing of children's personal data

SoBRA membership does not include ages 16 or under and its processing or ownership is not considered applicable.

Transferring your information outside of Europe

As part of the services offered to you through this website, the information which you provide to us may be transferred to countries outside the European Union ("EU"). By way of example, this may happen if any of our servers are from time to time located in a country outside of the EU. These countries may not have similar data protection laws to the UK. By submitting your personal data, you're agreeing to this transfer, storing or processing. If we transfer your information outside of the EU in this way, we will take steps to ensure that appropriate security measures are taken with the aim of ensuring that your privacy rights continue to be protected as outlined in this Policy.

Website recording

The SoBRA web site does not undertake recording of any kind. Webinars provided by third parties may be recorded by the host provider. Please refer to "Links to other websites" above.

Review of this Policy

SoBRA commit to keep this Policy under regular review. This Policy was last updated in May 2018. It is intended that it will be reviewed as a minimum annually.

Data Breach

The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the Information Comissioners Office (ICO) and, in some cases, to the individuals affected. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We have to notify the ICO of a breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay.

In all cases we must maintain records of personal data breaches, whether or not they are notifiable to the ICO.

We would report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. The GDPR recognises that it will not always be possible to investigate a breach fully within that time-period and allows us to provide additional information in phases, so long as this is done without undue further delay

Our internal breach reporting procedure will be reviewed annually. In light of the tight timescales for reporting a breach - it is important that we have robust breach detection, investigation and internal reporting procedures in place.

General Guidelines for SoBRA Members

- The only people able to access data covered by this policy should be those who need it for their work and delivering the interests of the individual and SoBRA.
- Data should not be shared informally.
- SoBRA will provide this guidance to its current Executive Committee, new committee members, accreditation scrutineers and website designer to help them understand their responsibilities when handling data.
- SoBRA representatives should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within SoBRA or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

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:

- 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. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- SoBRA representatives should not save 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 an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the SoBRA's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall. The Data protection officer is to annually document and update a listing of IT security measures.