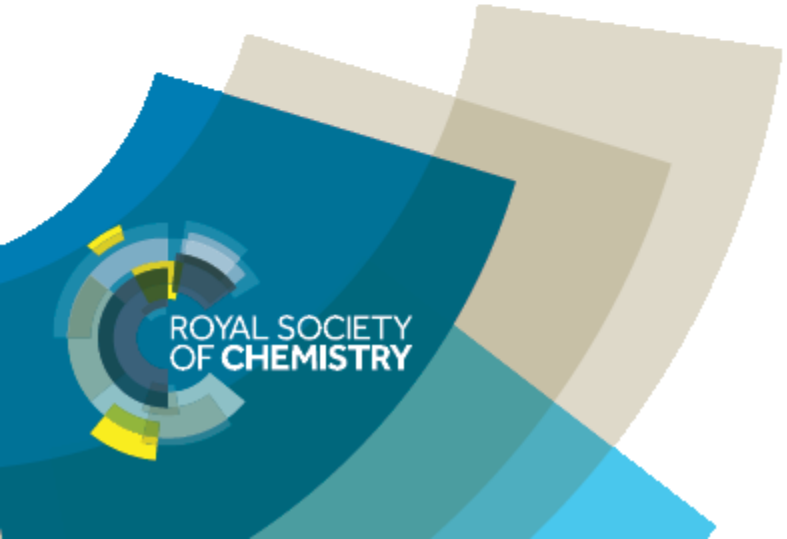
GDPR Guidelines
May 2018

ROYAL SOCIETY OF CHEMISTRY

Terminology



Data subject means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about.

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data

Personal data means any information relating to an identifiable natural person (**data subject**).

An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as:

- a name
- location data
- an online identifier
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

Sensitive Data

Termed **special categories of personal data** within GDPR.

Sensitive data consists of:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Sexual orientation/ sex life
- Genetic data
- Biometric data

Basis of processing

- **Legitimate interest** - processing is necessary for the purposes of the interests pursued by the RSC except where such interests are overridden by the fundamental rights and freedoms of the data subject.

- **Contract** – processing is necessary for the performance of a contract to which the data subject is party.

- **Consent** – when the data subject has given explicit consent to the processing of their personal data for one or more specific purposes.

Legitimate interest

- Legitimate interests is the most flexible lawful basis for processing, **but you cannot assume** it will always be the appropriate.

- Legitimate interest is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified. For example if someone attended a conference 2 years ago and you would like to invite them to the same conference again.

- Legitimate interest is different to the other lawful bases as it is not centered around a particular purpose (e.g. performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent). Legitimate interest is more flexible and could in principle apply to any type of processing for any reasonable purpose.

- Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances. This is different to the other lawful bases, which presume that your interests and those of the individual are balanced.

Legitimate interest continued

- You can rely on legitimate interest for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object.

- This can be broken down into a three-part test:

  Purpose test: are you pursuing a legitimate interest?

  Necessity test: is the processing necessary for that purpose?

  Balancing test: do the individual's interests override the legitimate interest?

- You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

Consent

- Where consent is the basis for processing, GDPR requires it to be freely given, specific, informed and unambiguous.
- Check your consent practices and your existing consents. Refresh your consents if they don’t meet the GDPR standard.
- Consent requires a positive opt-in. Don’t use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and ‘granular’ so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.

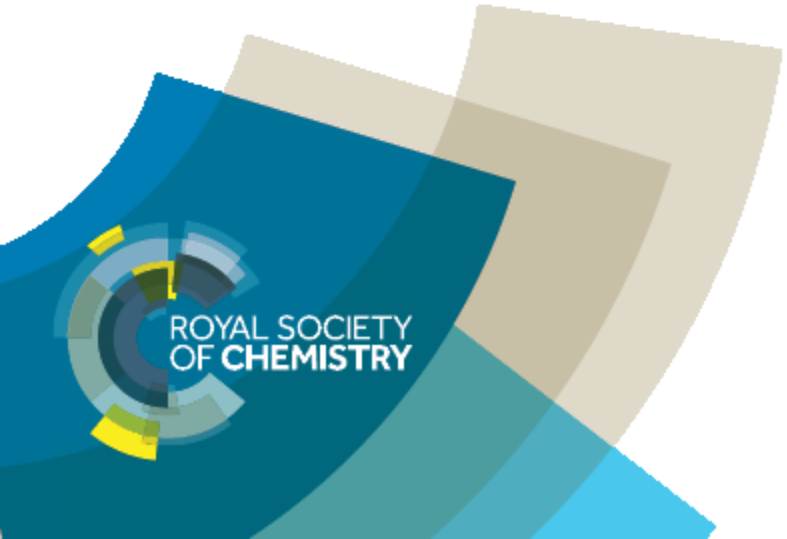
Subject Access Request (SARS)

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Should a member request right of access please inform the data protection officer at the RSC as soon as possible dpo@rsc.org.

Documents
Committee minutes
Delegate lists
Committees emails



- Any email addresses or contactable data for an individual featured in any committee meetings, AGM attendees lists, event delegate lists, event flyers/posters MUST be deleted. Names can remain.

- No committee should be processing children's data.

- Past award/prize winners emails and contactable data should be deleted.

- Any bursary/travel grant applications should be destroyed appropriately once the bursary/travel grant has been awarded and contactable details are no longer needed.

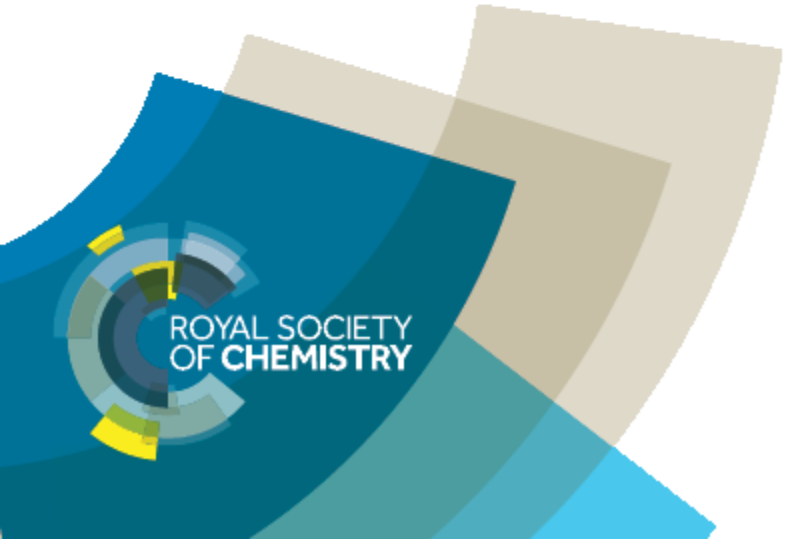
- Any contactable data that is kept by the committee (in line with GDPR) must be stored securely. Fines can be issued for loss of data and not storing data correctly.

- Any contactable data being shared (in line with GDPR) must be done securely. Fines can be issued for not sharing contact data securely.

- Ex-committee members contactable data must be deleted.

- Any contactable data obtained from the RSC must be deleted or destroyed once the purpose the data was requested for has been completed.

Events



Registration

- If using a third party it is the member groups responsibility to check that the third party is a registered data controller/processor and how they handle, store and delete data.

- When taking registrations for an event you must get consent for the following: passing registrants name and contact details to exhibitors and sponsors, taking and using photographs of registrant, what details they would like to be shared on the delegate list, if there is to be an electronic delegates list shared after the event.

- If you want to contact the registrant again about this event you must gain positive consent and keep this record of consent. You must have the date, the name and signature of the individual and a clear description of what communication the individual has signed up for.

- Information such as dietary requirements can be collected but must be deleted after the event.

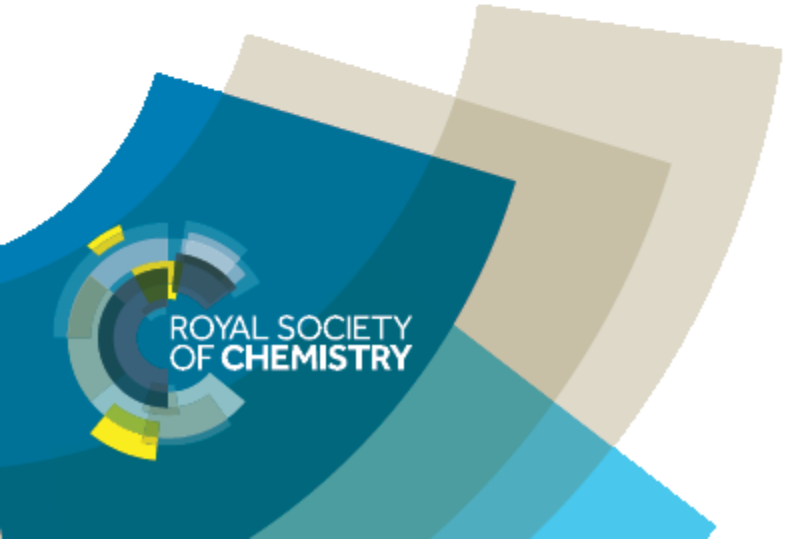
During an event

- There must be an identifier for those that do not want to be photographed, such as a coloured dot on a name badge.
- Any delegate lists left out after the event/day has ended must be collected in.
- Sign up sheets to hear about the conference/event again, must be clear in what the recipient will be receiving in terms of communication, there must be space for the delegates name, signature and date and it must be clear they are positively consenting to receive information about the conference/event.

After an event

- Any remaining delegate lists must be destroyed.
- Sensitive data such as dietary requirements must be deleted.
- There shouldn’t be a need to hold children’s data.
- Advertising of the same event must be recorded – what communication was sent, how it was sent, who it was sent to, if you had positive consent. This is for any audits.
- If using a third party check with them (if you haven’t done so already) when they will delete any data that doesn’t need to be kept.

E-alerts



E-alerts sent via RSC

- Our renewal sign up and new member sign up includes the new GDPR laws and therefore when a member joins or renews they have consented to hear from the RSC and any Interest Group of which they become a member.

- Ensure there is an unsubscribe option in all RSC sent e-alerts.

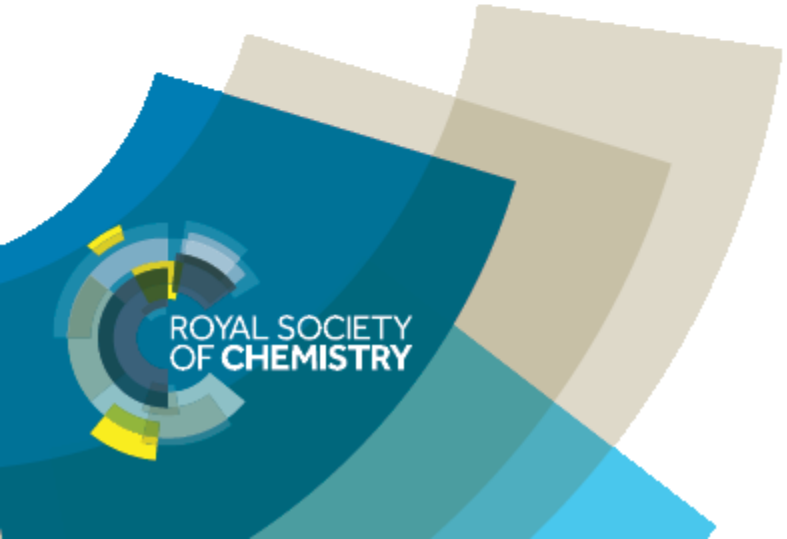
- E-alerts from other groups to your members should be reviewed on an email by email basis and only sent to your members if you believe there is legitimate interest, current arrangements between member groups will no longer stand and cannot be set up.

- E-alerts sent through the RSC will have an audit trail, this means we can show when an e-alert was sent, to who it was sent, by who it was sent and that there was permission to contact those individuals. All emails sent must have an audit trail.

E-alerts/emails sent via third parties

- Member groups must ensure that the third party is a registered data controller.
- **Please do not assume that 3rd parties/contractors are compliant - check!**
- There must be an unsubscribe option clearly displayed in the e-alert.
- An audit trail must be kept to show when the email was sent, who sent it, who it was sent to and consent from the individual that they wanted to received that email or that is was of legitimate interest to them.
- Emails can be sent to non-members on the following basis: legitimate interest (e.g. they attended the advertised conference for the last three years), you have their consent, you are fulfilling a contract.
- Contactable data must not be stored or kept by the third party once their contract has been fulfilled.
- The RSC data protection officer must be informed of any data breaches within 72 hours of the breach having occurred.

What to do in the event of a breach



What is a breach?

It means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processedAn incident includes but is not restricted to, the following:

- Loss or theft of personal data or equipment on which such data are stored (e.g. loss of laptop, USB storage device, iPad/tablet device, or paper record).
- Equipment theft or failure.
- Unauthorised use of, access to or modification of data or information systems.
- Attempts (failed or successful) to gain unauthorised access to information or IT systems.
- Unauthorised disclosure of sensitive/confidential data.
- Cyber attack.
- Unforeseen circumstances such as a fire or flood.
- Human error.
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

What to do if a breach occurs?

- A breach must be reported to the Data Protection Officer at the RSC without undue delay. The Data Protection Officer only has 72 hours to report the breach.

- The Data Protection Officer can be contacted by dpo@rsc.org, 01223 432258 or 07825 186304.

- If the breach occurs or is discovered outside normal working hours, it must still be reported to the DPO immediately.