Subject Access Request Policy

Individuals have the right to access and receive a copy of their personal data, and other supplementary information as detailed in our *Personal Data Processing Policies*.

Individuals can make Subject Access Requests (SARs) verbally or in writing, including via social media.

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

If an individual is making an SAR on the behalf of someone else YBSN need to satisfy that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority. The timescale for responding to an SAR does not begin until we have received any request to verify an individual's identity. However, this should be requested promptly.

Once YBSN has received an SAR we must respond to it within one month. If the request is complex, it can be extended to two months.

Any data that is given in a verbal response (after confirming their identity), will be recorded by date they made the request, the date we responded, details of who provided the information and the information we provided.

Exemptions

It is possible to refuse to provide all or some of the information we are required to provide to a person in response to their SAR if it falls under an exemption. This includes:

- confirmation that you are processing their personal information;
- a copy of their personal information; and
- other supplementary information.

If an exemption is considered necessary it will be applied on a case-by-case basis and documented and justified under the accountability principle.

If we refuse to comply with a request, we will inform the individual of:

- the reasons why

- their right to make a complaint to the controller
- their right to make a complaint to the ICO; and
- their ability to seek to enforce these rights through the courts.

In regard to the exemptions listed below the term 'prejudice' meaning may vary depending on the nature of the information, but in general it can mean:

- compromising or undermining a purpose or function;
- have a damaging or detrimental effect on what you are doing
- preventing a purpose or function from being carried out independently or fairly

Crime and taxation: general

Part one – personal information processed for the following crime – and taxation-related purposes:

- The prevention, investigation or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty, or an imposition of a similar nature.

Functions designed to protect the public

Personal information is exempt from the right of access if it's processed to perform one of six functions designed to protect the public, or if it relates to the actions of another organisation to carry out these functions — for example, if it's information:

- that you have shared with the other organisation; or
- that shows that the other organisation has contacted you about the person in relation to its investigations.

This exemption only applies if complying with the SAR would likely prejudice the performance of a specific functions or function.

The one of the four functions is to:

- protect the public against dishonesty, malpractice or other seriously improper conduct (or unfitness or incompetence);

When using this exemption YBSN must be able to show that one of the above functions is:

- conferred on a person by enactment;
- a function of the Crown, a Minister of the Crown or a government department; or
- of a public nature and exercised in the public interest.

When using exemptions from DPA 2018 it relieves YBSN from some of our obligations, for example:

- the right to be informed;
- the right of access;
- dealing with other individual rights;
- reporting personal data breaches; and
- complying with the principles.

The exemption only applies to the extent that complying with these provisions would be likely to prejudice YBSN's purposes of processing. If this is not so, YBSN must comply with the GDPR as normal. Most data held would not prejudice the crime purposes (e.g. date, time, place of incidents,) but disclosing say, the method used to carry out the offending behaviour or where property was disposed of, might prejudice the crime purposes.

Rights of Others

Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, they are not obliged to comply with the request unless:

- the other person has consented to the disclosure; or
- it is reasonable to disclose the information without their consent.

When deciding whether it is reasonable to comply with a request without the consent of another identifiable individual, the data controller must consider all relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality owed to the third party;
- any steps you have taken to try to get the third party's consent;
- whether the third party is capable of giving consent; and
- any stated refusal of consent by the third party.

The Commissioner takes the view that, for the exemptions to apply there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged. Partnerships should retain a written record of reasoning and evidence for applying any exemptions.