



Data Subject Contact Form – Frequently Asked Questions

What is personal data?

Personal data is information that can identify a person, either directly or indirectly. This may include name, address or location, contact details, online identifier, ID or passport number.

Under the General Data Protection Regulation (GDPR), there are special categories of personal data that require a higher level of protection such as information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health, sex life or sexual orientation. These types of data are referred to as *sensitive personal data*.

What is a data subject?

A data subject is a living person about whom personal data is being collected, held or processed. Data subjects can either be identified, whereby we know who they are, or identifiable, whereby we may be able to directly or indirectly identify them.

Am I a data subject of Ferring?

If you are an employee at Ferring, we are required to collect and process some categories of personal data about you. This is necessary for a range of purposes which include, for example, paying your salary or complying with legal employment obligations. This means that you are a *data subject* of Ferring.

Ferring data subjects may also include ex-employees, job applicants, doctors, patients, third party vendors and any other individuals about whom we collect, hold or process personal data.

Does Ferring have a Data Protection Officer?

Ferring has appointed a Global Data Protection Officer. You can contact the Global Data Protection Officer via the Data Subject Contact Form.

What is the Data Subject Contact Form?

The Data Subject Contact Form is an online portal available to all Ferring data subjects. Data subjects can use this form to:

- report a data incident or potential data breach;
- submit a request to exercise their rights as data subjects; and
- contact the Global Data Protection Officer.

How can I access the Data Subject Contact Form?

The Data Subject Contact Form is available via the Ferring Intranet Privacy page, or by visiting globalDPO-ferringus.ethicspoint.com.

Who operates the Data Subject Contact Form?

The Data Subject Contact Form is operated by NAVEX Global.

What is the difference between a *data incident* and a *personal data breach*?

Different types of incidents can occur affecting different types of data. The following definitions should help to explain these distinctions and how you may recognize a data incident or personal data breach:

Security incident: an event which indicates that the organization's systems, applications, networks, devices and/or data may have been compromised or that the security measures put in place to protect them may have failed

Security breach: a security incident which has resulted in the unauthorized access of the organization's systems, applications, networks, devices and/or data, by bypassing their underlying security mechanisms. Different levels and types of breaches may occur.

Data incident: an event which indicates that the organization's data may have been compromised or that the security measures put in place to protect those data may have failed.

Personal data breach: a data incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Examples of a data incident or personal data breach may include a lost or stolen laptop, an external hacker, an email containing personal data sent in error, documents left in an unsecured location, information lost in transit or employee misconduct in sharing personal data.

Why should I report a data incident or potential personal data breach?

Reporting such incidents immediately upon discovery will ensure vulnerabilities are detected quickly and the potential impact on any affected personal data is minimized. It will also ensure that Ferring is able, if required, to notify the relevant authority within the applicable time limit. Reporting will help us act quickly, minimize risk, protect our employees and meet our legal obligations.

Can I report a data incident or potential personal data breach anonymously?

Unfortunately, we are unable to accept an anonymous report of a data incident or potential personal data breach via the Data Subject Contact Form. Under the General Data Protection Regulation (GDPR), we have a legal obligation to notify certain personal data breaches to the competent supervisory authority within 72 hours; however, we will report as required by local law or applicable statute. We therefore have a short time period in which to determine if a personal data breach has occurred and whether it poses a risk to the rights and freedoms of the affected data subject(s). An anonymous submission would limit our ability to follow up and investigate the report. We do operate a zero-retaliation environment as stated in the Ferring Code of Conduct and the act of reporting a data incident should not incur consequences.

What are my rights as a data subject?

Data subjects may have specific rights under applicable data protection laws. These rights are not absolute and may be subject to a number of conditions and/or exemptions. Under the GDPR, these rights may include:

- **Right to access and rectification:** the right to request a copy of the information we hold about you, as well as the right to request the correction of the personal data we hold if it is inaccurate.
- **Right to erasure and restriction of processing:** the right to request the erasure of your personal data or for the restriction of processing your personal data. These rights are limited and will apply only in certain circumstances and where no exemptions apply.
- **Right to data portability:** the right to request a copy of the personal data we hold, as well as the right to request this data to be transferred to another controller. This right is subject to certain conditions and may not apply, for example, if not permitted for reasons of public interest, or is not technically feasible.
- **Right to object:** the right to object to the processing of your personal data. If the data is processed for reasons of public interest, scientific or statistical purposes, you may still object and it will be our responsibility to demonstrate the legitimacy of processing the data.
- You have the right to contact or lodge a complaint with your local data protection supervisory authority.

How can I exercise my rights as a data subject?

You may submit a request to exercise your rights as a data subject by selecting the applicable option on the Data Subject Contact Form.

Why might I be required to submit proof of my identity?

If you request a copy of the personal data we hold about you, we may be required to confirm your identity to ensure that we only release personal data to the verified data subject requesting it. You may therefore be asked to provide a document to prove your identity, before we release the data you have requested. Please refer to the Privacy Notice on the Data Subject Contact Form for more information.

Can I contact the Data Protection Officer on a general matter?

Yes, you may contact the Global Data Protection Officer for a matter unrelated to a data incident or your rights as a data subject.

When will I receive a response?

All submitted reports will be assessed upon receipt. You may use the follow up function on the Data Subject Contact Form to track the progress of your report.

Reports of data incidents will be responded to as a matter of priority depending on the severity of the report. Requests relating to data subject rights will be responded to as soon as possible, or by a timetable otherwise required by applicable law or local statute, but no later than 30 days after the submission of the form. General inquiries will be responded to within a reasonable timeframe.

Last updated 12th July 2019