



Privacy Policy

(This document is for Internal use only)

Streamlined Forensic Reporting Limited

To request a change to this document template, contact the document author or owner. Copyright © 2023 SFR medical Limited.

Table of Contents

1. IMPORTANT INFORMATION.....	2
1.0 PURPOSE OF THIS PRIVACY POLICY.....	2
1.1 CONTROLLER.....	2
1.2 CHANGES TO THE PRIVACY POLICY AND YOUR DUTY TO INFORM US OF CHANGES.....	2
1.3 THIRD-PARTY LINKS.....	2
1.4 THE DATA WE COLLECT ABOUT YOU.....	3
1.5 IF YOU FAIL TO PROVIDE PERSONAL DATA.....	3
1.6 HOW IS YOUR PERSONAL DATA COLLECTED?.....	3
2. HOW WE USE YOUR PERSONAL DATA.....	4
2.0 PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA.....	4
2.1 MARKETING.....	5
2.2 COOKIES.....	6
2.3 CHANGE OF PURPOSE.....	6
2.4 DISCLOSURES OF YOUR PERSONAL DATA.....	6
3. INTERNATIONAL TRANSFERS.....	6
4. DATA SECURITY.....	7
5. DATA RETENTION.....	7
5.0 HOW LONG WILL YOU KEEP MY PERSONAL DATA FOR?.....	7
5.1 YOUR LEGAL RIGHTS.....	8
5.2 NO FEE USUALLY REQUIRED.....	8
5.3 WHAT WE MAY NEED FROM YOU.....	8
5.4 TIME LIMIT TO RESPOND.....	9
6. GLOSSARY.....	9
7. VALIDITY AND DOCUMENT MANAGEMENT.....	9
8. VERSION CONTROL.....	9

Note: You can print this document. Please use the glossary to understand the meaning of some of the terms used in this Privacy Policy.

1. IMPORTANT INFORMATION

1.0 Purpose of this Privacy Policy

Streamlined Forensic Reporting Limited (also referred to as SFR Medical) respects your privacy and is committed to protecting your personal data. This Privacy Policy will inform you how we collect, process, and/or store your personal data when you engage with us, both on- and off-line, tell you about your privacy rights and how the law protects you. This is applicable, but not limited to those who are looking for more information about Streamlined Forensic Reporting Limited, potential or current clients, and victims who are subjects of SFR medical reports and their family members.

We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us. This website is not intended for children and we do not knowingly collect data relating to children online. When appropriate and consent has been given, we do collect data about children who are subjects of an SFR medical report.

It is important that you read this Privacy Policy together with any other policies we may provide on specific occasions when we are collecting or processing personal data about you, so you are fully aware of how and why we are using your data. This Privacy Policy supplements other notices and policies and is not intended to override them.

1.1 Controller

Streamlined Forensic Reporting Limited is the processor for requests made by the Police, and controller for any other information and responsible for your personal data (collectively referred to as Streamlined Forensic Reporting Limited, "we", "us" or "our" in this Privacy Policy).

If you have any questions about this Privacy Policy, including any requests to exercise your legal rights, please contact us:

- Full name of legal entity: Streamlined Forensic Reporting Limited
- Email address: contact@sfrmedical.com
- Telephone number: 01234943111, option 3

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

1.2 Changes to the Privacy Policy and your duty to inform us of changes

We keep our Privacy Policy under regular review. This version was last updated on 1st June 2023.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

1.3 Third-party links

This website and emails we may send you may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites or businesses and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

1.4 The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity data** includes your first and last name, job title, Twitter handle, Facebook profile, biography, and business association.
- **Incidence data** includes a date and location of incidence, date of hospital or GP visit, examination time, DOB, gender, date of discharge, and a summary of the medical examination which may include additional details around the incident itself.
- **Contact data** includes a billing address, delivery address, email address and telephone numbers .
- **Financial data** may include bank account details.
- **Transaction data** includes details about payments to and from you and other details of products and services you have purchased from us or we have purchased from you.
- **Technical data** includes device type, browser type and version, time zone setting and location, language, gender, age, browser plug-in types and versions, operating system and platform.
- **Profile data** includes information similar to your identity data plus contact information along with any requests you may have made to us.
- **Usage data** includes information about how you use our website, products and services.
- **Marketing and communications data** includes your preferences to not receive marketing from us.

We also collect, use and share **aggregated data** such as statistical or demographic data for any purpose. Aggregated data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your usage data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Policy.

We may collect **special categories of personal data** about you (including details about your health, race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and/or genetic and biometric data) as part of our processing requirements for our clients (Police Forces).

1.5 If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel a product or service you have with us, but we will notify you if this happens.

1.6 How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions:** You may give us the data referenced above by filling in forms or corresponding with us by post, phone, email or otherwise. This includes data you provide when you:
 - o contract with us for our products or services
 - o utilise our service
 - o are the victim of a crime and have signed a consent form
 - o request marketing materials to be sent to you

- o give us feedback or contact us
- **Automated technologies or interactions:** When you interact with our website, we use Google Analytics to automatically collect technical data about your equipment, browsing actions and patterns.
- **Third parties or publicly available sources:** We may receive personal data about you from various third parties and public sources, including but not limited to those listed below:
 - o police forces
 - o victim signed consent form(s), shared by a police force
 - o hospitals and/or doctors
 - o hospital and/or police websites and/or FOIA requests
 - o news media
 - o social media channels
 - o analytics providers
 - o advertising networks
 - o search information providers

2. HOW WE USE YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- where we need to execute against a contract we are about to enter or have entered into with you
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests
- where we need to comply with a legal obligation

You have the right to withdraw consent at any time by contacting us.

2.0 Purposes for which we will use your personal data

Below is a description of the ways in which we may use your personal data, and of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground, we are relying on to process your personal data.

Purpose (activity)	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new client	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order with may include: (a) managing payments, fees and charges (b) collecting money owed to us (c) delivering SFR medical statements	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)

Purpose (activity)	Type of data	Lawful basis for processing including basis of legitimate interest
To manage our relationship with you which may include: (a) contacting you for more information (b) requesting a referral (c) following up on a previous request	(a) Identity (b) Contact (c) Profile (d) Marketing and communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To enable you to partake in a prize draw, competition or complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business re-organisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you, either on this website or through our social media channels	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and communications (f) Technical (g) Medical	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and communications	Necessary for our legitimate interests (to develop our products/services and grow our business)

2.1 Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. Please contact us for additional information.

- Promotional offers: we may use your identity, contact, technical, usage and profile data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant to you. You may receive marketing communications from us if you have requested information from, or contracted with, us and you have not opted out of receiving these materials
- Third-party marketing: we will get your express opt-in consent before we share your personal data with any third party for marketing purposes.
- Opting-out: you can ask us or third parties to stop sending you marketing messages by contacting us at any time.

Where you opt-out of receiving these marketing messages, this will not apply to personal data provided to us as a result of Streamlined Forensic Reporting Limited providing contracted services to police forces which is the basis of our business.

2.2 Cookies

Cookies are enabled on our website, specifically ones from Google, Facebook and Doubleclick.net. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies.

2.3 Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

2.4 Disclosures of your personal data

We may share your personal data with the parties below for the purposes set out above:

- internal and/or external third parties listed in the glossary
- specific third parties to whom we may choose merge parts of our business or our assets; alternatively, we may seek to acquire other businesses or merge with them

If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law.

We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

3. INTERNATIONAL TRANSFERS

We may share your data with authorised Streamlined Forensic Reporting Limited staff and other service providers on a need-to-know basis. This may involve transferring your data outside the European Economic Area (EEA).

We ensure your personal data is protected by requiring everyone to follow the same rules when processing your personal data. These rules are called "binding corporate rules". For further details, see European Commission: Binding corporate rules.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of personal data to third countries
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between Europe and the US. For further details, see European Commission: EU-US Privacy Shield

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

4. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

5. DATA RETENTION

5.0 How long will you keep my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Details of retention periods for different aspects of your personal data are available in our retention policy which you can request from us by contacting us. In some circumstances you can ask us to delete your data: see your legal rights below for further information.

In some circumstances we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

5.1 Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data:

- **Request access to your personal data:** commonly known as a "data subject access request". This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
 - **Request correction of your personal data that we hold about you:** this enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
 - **Request erasure of your personal data:** this enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
 - **Object to processing of your personal data of your personal data:** if we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
 - **Request restriction of processing your personal data:** this enables you to ask us to suspend the processing of your personal data in the following scenarios:
 - o if you want us to establish the data's accuracy;
 - o where our use of the data is unlawful but you do not want us to erase it
 - o where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - o you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it
 - **Request transfer of your personal data to you or to a third party:** we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
 - **Right to withdraw consent at any time:** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.
- If you wish to exercise any of the rights set out above, please contact us.

5.2 No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive.

5.3 What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to

access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

5.4 Time limit to respond

We try to respond to all legitimate requests within 30 business days. Occasionally it could take us longer if your request is particularly complex or you have made several requests. In this case, we will notify you and keep you updated.

6. GLOSSARY

- **SFR medical report:** a Streamlined Forensic Report, the medical evidence which Streamlined Forensic Reporting Limited provides to the police after a crime has taken place, at the request of a police officer
- **Consent form:** the form victims sign which gives Streamlined Forensic Reporting Limited access to their personal, medical, and other data for the purpose of writing an SFR medical report
- **Legitimate interest:** the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience
- **Performance of contract:** the processing your data where it is necessary to be able to fulfill a contract to which you are a party or to take steps at your request before entering into such a contract
- **Comply with a legal obligation:** if required, we will process your personal data in a way that is compliant with and adheres to the relevant law(s)
- **Internal third parties:** other entities in Streamlined Forensic Reporting Limited (acting as joint controllers or processors) based outside the EEA (in but not limited to India, South Africa, and the US) who provide IT and system administration, SFR processing and report writing, operational, marketing, and leadership services
- **External third parties:** includes the following:
 - o service providers acting as processors, based India, Canada, and the US who provide IT and system administration services
 - o professional advisers, acting as processors or joint controllers including lawyers, bankers, auditors, funding sources, and insurers based in the UK and India who provide consultancy, banking, legal, insurance and accounting services
 - o HM Revenue & Customs, regulators, and other authorities, acting as processors or joint controllers, based in the UK who require reporting of processing activities in certain circumstances
 - o police forces and other criminal justice partners (including CPS and hospitals), acting as processors or joint controllers, based in the UK

7. VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of January 13, 2023.

The owner of this document is Compliance officer, who must check and, if necessary, update the document at least every 6 months.

8. VERSION CONTROL

CHANGE LOG

Created by:	Johann Grundlingh
Approved by:	Suyash Shrivastava

<i>Date</i>	<i>Version</i>	<i>Created by</i>	<i>Description of change</i>
	1.0	Johann Grundlingh	Initial version
13-01-2023	2.0	Samriddhi Shrivastava	Updated version
13-01-2023	2.1	Johann Grundlingh	Updated version with details about special category data and Data Processor agreements.