SUSPECTED ADVERSE EVENT PRIVACY NOTICE

1. INTRODUCTION

CSL Limited and its affiliates ("we", "us", "our", "CSL") are committed to protecting your privacy. When a suspected adverse event concerning one of our medicinal products is reported to us, we will collect certain information that can be used to identify you ("**personal data**").

The marketing authorisation holder of the medicinal product is the "data controller" of the personal data we collect in relation to reporting suspected adverse events concerning one of our medicinal products. This means that the marketing authorisation holder is responsible for decisions about the collection and use of personal data. It also means they are responsible for responding to your questions and requests in relation to the personal data we hold about you.

By contacting privacy@cslbehring.com, we can assist you in identifying the CSL affiliate which is the marketing authorisation holder for the medicinal product you may have concerns about.

This privacy notice explains how the marketing authorisation holder uses the personal data they receive in connection with a suspected adverse event. It also explains your rights in relation to your personal data.

2. WHO DOES THIS PRIVACY NOTICE APPLY TO?

This notice applies to you if you are:

- identified in a report as being impacted by a suspected adverse event; or
- you are making a suspected adverse event report on the behalf of someone else (and you identify yourself to us when making that report).

3. CATEGORIES OF PERSONAL DATA WE COLLECT

We may collect the following categories of personal data in relation to a suspected adverse event:

- **Contact and identification data** such as your name, home address, telephone numbers, email addresses, gender, citizenship, date of birth, health insurance or patient number;

- **Relevant health and sensitive data** such as existing or previous health or medical conditions, (including disabilities or diseases), medication you are taking, genetic data, biometric data, blood type, vaccinations you may have had, allergy information, ethnicity, drug use and sexual orientation and history.

Sensitive data generally means any information about you that is particularly sensitive or private or could be used in a discriminatory way. As a result, we need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the circumstances listed in section 5 below. .

4. HOW WE COLLECT YOUR PERSONAL DATA

We collect personal data directly from you when you report a suspected adverse event directly to us. This could be by way of adverse event reporting forms, questionnaires, interviews or observations we make about you and your health after a suspected adverse event has been reported to us.

We may also collect personal data about you indirectly from third parties when they report a suspected adverse event. This could include reports from your doctor or other healthcare professionals, a distributor of our products, any other entity within our company group (when they receive adverse event information) or any person (such as a family member or friend) who reports an event on your behalf.

5. PURPOSES YOUR PERSONAL DATA IS USED FOR

In the below table, we describe the:

- purposes we collect and use your personal data for;
- categories of personal data we collect for those purposes; and
- legal basis that allows us to collect and use your personal data.

Purpose of personal data use	Categories of personal data we use	Legal basis for using the personal data
Identifying and contacting you	Contact and identification data.	Legitimate interests: We will use your personal data for the legitimate interest we have in assessing our products performance and safety and meeting our industry and regulatory obligations. Provision of health care: We will use your personal data where it is needed for the provision of health care or treatment. Legal obligations: We will use your personal data to meet legal obligations we are subject to with respect to suspected adverse event reporting. Vital interests: We will use your personal data to protect your vital interests, or the vital interests of other individuals that may be impacted by the suspected adverse event. Public interest: We will use your personal data where it is needed in the public interest, such as protecting against serious threats to health and ensuring high standards of our medicinal products and related healthcare.
Collection, examination and storage of suspected adverse event information	Contact and identification data. Relevant health and sensitive data.	
Communicating information about a suspected adverse event to relevant parties (such as heath regulators)	Contact and identification data. Relevant health and sensitive data.	

6. HOW WE WILL KEEP YOUR DATA SECURE

We have put in place appropriate security measures to prevent your personal data from being accidentally lost or used, accessed, altered or disclosed in an unauthorised way.

In addition, we limit access to your personal data by our employees and service providers, to individuals who have a legitimate need to know for the job or service they provide to us. They will only process your personal data on our instructions and are required to keep your personal data confidential.

We have put in place procedures to deal with suspected data security breaches and will notify you and any applicable regulators of breaches in accordance with relevant legal requirements.

7. HOW LONG WE WILL KEEP YOUR PERSONAL DATA FOR?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal or reporting requirements.

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, whether we can achieve those purposes through other means and the applicable legal requirements.

We will typically keep your personal data in relation to suspected adverse events to our medicinal products for up to 10 years after the expiration of our marketing authorisation for the relevant medicinal products. However, if there are legal obligations for us to keep the data for longer we may do this.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you.

8. WHO HAS ACCESS TO YOUR PERSONAL DATA?

- **Our staff –** your personal data will be accessed by our staff but only where this is necessary for their job role.
- **Companies in our group –** we will share personal data with other companies in our group but only where this is necessary for the purpose of assessing and responding to the suspected adverse report to ensure we are taking appropriate action to protect health.
- **Third parties that process personal data on our behalf –** third party service providers (such as Pharmacovigilance service providers, data storage providers, data analytics providers and IT technical support) who process personal data as part of providing a service to us, may also have access to your personal data. They will be required to keep your personal data secure and will not be allowed to use your personal data for their own purposes.
- **Third parties that provide us with your personal data when making a report –** third parties (such as doctors or other healthcare professionals, distributors of our products or any person who reports an event on your behalf) may receive personal data from us as we communicate with them about the adverse event report they have made. We will only share your personal data with these parties where we need to do this to meet our regulatory and industry obligations with respect to responding to suspected adverse event reports.
- **National health authorities or other health regulators –** where we are required to notify national health authorities or other health regulators about adverse reactions to our medicinal products, we will share personal data with them for that purpose. The national health authorities or other health regulators will become independent controllers of the personal data we transfer to them. They will use the personal data for the purposes described above and their own privacy notice will apply to the use of the personal data they hold.

9. DO WE TRANSFER YOUR PERSONAL DATA OUTSIDE OF EUROPE?

In order to process your personal data for the purposes set out in this notice, we may transfer your personal data to third parties and other companies in our group which are based outside of the United Kingdom, Switzerland, the European Union and the European Economic Area (”**Europe**”).

To ensure that your personal data is secure, we will only transfer your information to countries outside of Europe where we do so in accordance with the EU’s General Data Protection Regulation (”**GDPR**”). This requires that one of the following conditions applies:

- the European Commission has decided that the country provides an adequate level of protection for your personal data (in accordance with Article 45 of the GDPR);
- the transfer is subject to a legally binding and enforceable commitment on the recipient to protect the personal data (in accordance with Article 46 of the GDPR);
- the transfer is made subject to binding corporate rules (in accordance with Article 47 of the GDPR); or
- the transfer is based on a derogation from the GDPR restrictions on transferring personal data outside of the EU (in accordance with Article 49).

10. WHAT RIGHTS DO YOU HAVE?

Under certain circumstances you have the right to:

- **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 the personal data that we hold about you. This enables you to have any incomplete or inaccurate personal data we hold about you corrected.
- **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 exercised your right to object to processing (see below).
- **Object to processing** of your personal data where 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.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you under certain circumstances, for example if you want us to restrict processing while the accuracy of the personal data is being established.
- **Request not to be subjected to automated decision-making**. However, we do not use automated decision-making or profiling as part of our business operations in relation to suspected adverse event reporting.

You can exercise your rights by contacting us using the contact details at the end of this notice. We will always aim to help you when you wish to exercise your rights but in some instances we may have lawful grounds to reject your request.

We will investigate any request you make immediately and will respond to you within a month of your request. That period may be extended by us for a further two months where this is needed to help us respond properly (for example if the request is complicated for us to deal with and we need more time) but we will let you know the reasons for the delay.

If we decide to not take action on the request, we will inform you of the reasons for not taking action.

If you do not agree with a decision we make in relation to a rights request or believe that we are in breach of data protection laws in the Europe, then you can lodge a complaint with a data protection regulator in Europe.

11. CONTACT US

If you require assistance in identifying the company which is the marketing authorisation holder, have any questions about how we process your personal data or want to exercise one of your rights, you can contact us or our Data Protection Officer using the following details: privacy@cslbehring.com

Or, via the CSL rights portal: https://privacyinfo.csl.com/

Last updated: February 2022