Almus Post-Marketing Pharmacovigilance Privacy Notice

Effective Date: [25 May 2018]

Almus Pharmaceuticals Limited ("**Almus**," **we**," "**us**," or "**our**") is committed to respecting your privacy. We developed this Post-Marketing Pharmacovigilance Privacy Notice ("**privacy notice**") in order to be transparent about the data we collect about you in connection with post-marketing drug safety and pharmacovigilance ("**PV**") activities, how this information is used and shared, and the choices and rights available to you with respect to the data we maintain about you.

This privacy notice applies to PV-related data processed in the post marketing setting only. Processing activities performed as part of a clinical trial or other Almus activities where you provide explicit consent for processing your personal data, as well as processing in connection with the secondary use of data for medical research, are not subject to this privacy notice.

Almus is the data controller with respect to the data processing activities described in this privacy notice. The contact details for Almus and its data protection officer are provided in the How to Contact Us section below.

I. Information We Collect and How We Use It

We collect or process information that either directly identifies you or could reasonably be used in combination with other information to identify you (we refer to this type of data as "**personal data**"). We collect your personal data when you provide it to us directly (*for example*, if you report an adverse event and provide us with your name or contact information); and when it is shared with us by reporters of adverse events or healthcare professionals (*for example*, when a healthcare provider shares personal data about a patient with us in connection with an adverse event report). The personal data collected by Almus in connection with post-marketing pharmacovigilance activities and the ways we use such data are described below.

- **Patients**. We collect and process personal data (including sensitive personal data) about patients who experience actual or suspected adverse events. Personal data about patients may include:
  - **Patient identifiers**, including the patient's initials, assigned ID, date of birth, age/age group, gender, weight, height or ethnicity, or a combination of any of the foregoing. We use this information to comply with regulatory obligations to report suspected adverse events and to identify duplicate events and related reports.
  - **Health information**, including the patient's medical history and health status, and medicinal products taken by the patient. We use this information to comply with regulatory obligations to report suspected adverse events and for effective safety data analysis and surveillance, including to help us understand more about the risks and benefits of a given product and to enhance the safety of patients.
  - **Event information**, including information about the adverse event or other special safety situation (*e.g.*, pregnancy, breast feeding, overdose, interactions, product abuse/misuse, medication error, unapproved/off-label use, occupational exposure, or lack of therapeutic effect), and other information to describe the course and outcome of the event (*e.g.*, details of symptoms, severity, duration, treatment and what medical attention (if any) was sought). We use this information to comply with regulatory obligations to report suspected adverse events and for effective safety data analysis and surveillance, including to help us understand more about the risks and benefits of a given product and to enhance the safety of patients.
- **Reporters**. We collect and process personal data about reporters of actual or suspected adverse events, such as the patient's healthcare provider, family member, or the patient themselves. Personal data about adverse event reporters may include the reporter's name, occupation or title, address, telephone number, email address, or other contact details. We use this information to comply with regulatory obligations to report suspected adverse events and to perform effective follow-up to ensure that complete and accurate PV data is collected and analyzed (*e.g.*, we may use

a reporter's contact information to obtain additional information about the event reported as part of our safety analysis).

In addition to the purposes for processing patient and reporter data identified above, we use personal data about patients and reporters as necessary to respond to law enforcement requests and as otherwise required by applicable law, court order or governmental regulations.

We processes personal data about patients and reporters for the foregoing purposes as necessary in order to comply with Almus' legal obligations, including post-marketing drug safety and pharmacovigilance reporting obligations. To the extent a given processing activity is not expressly required under applicable law, such processing is performed as necessary for Almus' legitimate interests and the interests of patients generally (namely, the enhancement of patient safety). With respect to the processing of sensitive personal data about patients, such processing is necessary for the purposes of preventive medicine and for reasons of public interest in the area of public health.

II. How Personal Data is Shared

We disclose your personal data to third parties who provide us with various business services, such as PV vendors who assist us with collecting adverse event information and compiling and submitting adverse event reports, or hosting providers that store personal data on our behalf. These service providers and contractors are restricted from using this data in any way other than to provide services for us and subject to our documented instructions only. Before sharing personal data with such providers, personal data is pseudonymized where appropriate or required by applicable law.

When submitting adverse event reports as required by law, we disclose personal data contained in such reports to applicable health authorities, including the European Medicines Agency (EMA). In addition, where required pursuant to applicable law or regulator instructions, we share personal data with licensing partners in order for such licensing partners to fulfil their respective PV-related compliance obligation in relation to a particular product. Only information which the licensing partners reasonably need and which is consistent with the purpose of PV is transferred. Further, these licensing partners are subject to the same confidentiality obligations as Almus with respect to the information we provide to them, and they may only process such information as necessary to satisfy their PV-related legal obligations.

In the U.K., we share personal data with the relevant marketing authorization holder in order for such authorization holder to satisfy its PV-related legal obligations. Only information which the holder reasonably needs and which is consistent with the purpose of PV is transferred. Before sharing personal data with the relevant marketing authorization holder, personal data is pseudonymized where appropriate or required by applicable law.

In addition, we may disclose personal data to third parties in special cases, including when we have a reason to believe that such disclosure is necessary to identify, contact or bring a legal action against someone who may be causing injury to or interference with our rights and property or those of any other person. We may also disclose your personal data when we believe the law requires it and in any situation that involves threats to any person's physical safety. This includes, but is not limited to, disclosures to law enforcement personnel or government agencies and authorities.

Personal data maintained by Almus is not transferred to or accessible by persons or entities outside the European Economic Area.

III. Your Rights

The rights available to you with respect to the processing activities covered under this privacy notice are described below. We reserve the right to limit these rights at any time where permitted under applicable law, including where your identity cannot be reasonably verified. To exercise any of these rights, please contact Almus using the contact information below.

Access Right

You have the right to obtain confirmation as to whether or not your personal data is being processed. Where it is processed, you have the right to access the relevant personal data and obtain 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. Where personal data is transferred to a third country or to an international organization, you shall have the right to be informed of the appropriate safeguards pursuant to GDPR relating to the transfer;
- 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 Almus rectification or erasure of personal data or restriction of processing of your personal data or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from you, any available information as to its source; and
- the existence of solely automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.

This privacy notice is intended to provide all of the information above. Any questions about these details may be directed to Almus using the contact information below.

Right to Rectification

You have the right to obtain from Almus without undue delay rectification of any personal data that is inaccurate or incomplete, including by means of providing a supplementary statement.

Right to Erasure

You have the right to have your personal data erased without undue delay where one of the following grounds applies:

- your personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- you object to the processing where such processing is based on the legitimate interest of Almus (or a third party) and there are no overriding legitimate grounds for the processing; or
- your personal data must be erased for compliance with a legal obligation in EU or Member State law.

This right to erasure shall not apply to the extent the processing is necessary for:

- compliance with a legal obligation which requires processing by EU or Member State law to which Almus is subject; or
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, to the extent permitted under applicable law.

Right to Restriction of Processing

You have the right to obtain from Almus restriction of processing of your personal data where one of the following applies:

- the accuracy of the personal data is contested;
- the processing is unlawful and you oppose the erasure of your personal data and request the restriction of its use instead;
- Almus no longer needs the personal data for the purposes of the processing, but it is required by you for the establishment, exercise or defense of legal claims; or
- where the processing is based on the legitimate interest of Almus (or a third party) and you have objected to processing.

Right to Object

You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data where such processing is based on the legitimate interest of Almus (or a third party). Almus will no longer process your personal data unless Almus demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

Right to File a Complaint

You have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work, or place of an alleged infringement if you consider that the processing of your personal data infringes applicable EU data protection laws.

IV. How We Protect Personal Data

Almus implements and maintains reasonable and appropriate technical, physical and organizational measures to protect personal data in accordance with applicable law. These measures include, but are not limited to, the following:

- Access to personal data is limited to authorized employees and service providers who need access to perform the activities described in this privacy notice on our behalf.
- Personal data is pseudonymized where appropriate or required by law.
- Almus personnel engaged in the processing of personal data are informed of the confidential nature of personal data, have received appropriate training on their responsibilities, and are obligated pursuant to Almus policy to maintain the confidentiality of personal data.
- The effectiveness of Almus security measures are regularly tested, assessed, and evaluated to ensure the ongoing security of processing systems.
- Internet-connected databases containing personal data are monitored for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms.
- Service providers and other third parties engaged by us to process personal data on our behalf are contractually obligated to process personal data only on our documented instructions and must provide similar security measures as those used by Almus and as required under applicable law.

Although we strive to provide reasonable and appropriate security for the personal data we process and maintain, no security system can prevent all potential security breaches. In particular, email or forms sent using our website or other online services may not be secure. You should take special care before deciding to send us information via email.

V. Retention and Deletion of Personal Data

Almus implements and maintains reasonable restrictions on the retention of personal data and generally disposes of such personal data once it is no longer necessary for the purposes for which it was collected or further processed. Generally, personal data contained in product-related documents is retained for as long as the marketing authorization (MA) exists and for at least 10 years after the MA has ceased to exist. However, we may continue to store archived copies of your personal data for legitimate business purposes and as necessary to comply with the law. In addition, we may continue to store anonymous or anonymized information for any legitimate business use described in this privacy notice.

VI. How to Contact Us

If you have any questions about this privacy notice, our use of your personal data in connection with post-marketing drug safety and pharmacovigilance, or your rights with respect to such use, you may contact us using the contact information below:

Almus

[**Almus Pharmaceuticals Limited**]

Data Protection Officer

[**Peter Sinfield**]

[2 The Heights]
[Brooklands]
[Weybridge]
[Surrey KT13 0NY]
[United Kingdom]
[Pharmacovigilance@almus.co.uk]

[Sedley place, 4th Floor]
[361 Oxford Street]
[London W1C 25L]
[United Kingdom]
[peter.sinfield@wba.com]

VII. Changes to Our Privacy Notice

Almus reserves the right to amend this privacy notice at our discretion and at any time. When changes are made to this privacy notice, the updated notice will be posted on our website, and will be effective as of the date posted. *Your continued use of our website or provision of PV data following the posting of changes will constitute your acceptance of such changes*. Material revisions to this privacy notice will not be applied retroactively without your affirmative consent.