



PRIVACY POLICY

Adopted 8th March 2019

Updated 6th September 2019

1. IMPORTANT INFORMATION AND WHO WE ARE

1.1 Purpose of this privacy policy

This privacy policy aims to give you information on how Oncimmune collects and processes your personal data and how we comply with European Union data protection requirements.

It is important that you read this privacy policy together with any other consent, privacy policy or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

1.2 Controller

Oncimmune is made up of different legal entities, details of which can be found below. This privacy policy is issued on behalf of the Oncimmune Group so when we mention "Oncimmune", "we", "us" or "our" in this privacy policy, we are referring to the relevant company in the Oncimmune Group responsible for processing your data.

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, please contact the data privacy manager using the details set out below.

Data Privacy Manager

Name: Dr Phil Gunning

Email address: phil.gunning@oncimmune.co.uk

Postal address: Clinical Services Building, City Hospital, Hucknall Road, Nottingham NG5 1PB

Changes to the privacy policy and your duty to inform us of changes

This version was last updated on 6th September 2019.

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.

2. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual which enables a person to be identified (directly or indirectly). It does not include data where the identity has been properly and irreversibly removed (anonymous data).

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

Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

Contact Data includes billing address, delivery address, email address and telephone numbers.

Financial Data includes bank account and payment card details.

Transaction Data includes details about payments to and from you and other details of products and services you have purchased from us.



Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.

Patient Story Data includes Identity Data, your background, ill-health study and testing experiences, treatment impacts, Special Category Data relating to your health, diagnosis and treatment as well as photo images and video clips when providing your feedback.

Profile Data includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

Special Categories of personal data is defined under the law as including data related to health, race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Usage Data includes information about how you use our website, products and services.

Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We may from time to time use personal data and convert it into anonymous data, to create higher level non-individualised analysis. We also collect, use and share such **Aggregated Data** such as statistical or demographic data for specific purposes including for research and statistical purposes. Aggregated Data may be derived from your personal data but is not considered personal data if the compiled or combined dataset does **not** directly or indirectly reveal your identity.

We may also collect Special Categories of personal data about you. We will only process Special Categories of personal data about you with your explicit consent, which may be withdrawn at any time, or if there is an alternative lawful basis.

We do not collect any information about criminal convictions and offences or personal data relating to children.

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 (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

3. 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 your Identity, Contact, Financial Data and Patient Story Data by filling in forms or by corresponding with us by post, phone, email, in connection with meetings, patient interviews or otherwise. This includes personal data you provide when you:

- apply for our products or services;
- request marketing to be sent to you;
- give us some feedback (including pharmacovigilance); or
- agree to participate in patient story exercises.

Automated technologies or interactions. As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.

Third parties or publicly available sources. We may receive personal data about you from various third parties and public sources as set out below:

Technical Data from the following parties: (i) analytics providers; (ii) advertising networks; and (iii) search information providers.

Contact, Financial and Transaction Data from providers of technical, payment and delivery services.



Identity and Contact Data from data brokers or aggregators.

Identity and Contact Data from publicly available sources such as Companies House and the Electoral Register based inside the EU.

4. 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 perform the contract we are about to enter into 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 or regulatory obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time.

Purposes for which we will use your personal data

We have set out in the table on the following page, a description of all the ways we plan to use your personal data, and which 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.



Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(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)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(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 produce patient stories demonstrating the experiences and success of a study, diagnosis or treatment for our, and the relevant study commissioning partner's business and promotional purposes.	(a) Patient Story	(a) Explicit consent
To administer and protect our business	(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 reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(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) Technical (b) Usage	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	Necessary for our legitimate interests (to develop our products/services and grow our business)



Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us

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 for you (we call this marketing).

You will receive marketing communications from the relevant group company] if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any third party company including those outside the Oncimmune group of companies for marketing purposes.

Opting out

You can ask us or third parties to stop sending you marketing messages at any time. In relation to third parties, you will need to contact them directly and in relation to our marketing, by contacting our Data Privacy Manager or following the opt-out links on any marketing message sent to you.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of, and necessary in relation to the delivery of a contract between us, product/service purchase, warranty registration, product/service experience, complaints or other transactions.

Withdrawing your consent in relation to your use of data in Patient Stories

You can revoke your consent in relation to our publication of patient stories before the information has been published, or sent to a publisher, or uploaded to the internet or published in any other way.

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 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, in certain limited circumstances, 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.

5. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties set out below for the purposes set out in the table on the previous page.

Oncimmune Ltd, Oncimmune Holdings plc, Oncimmune LLC, Oncimmune Germany GmbH

Company Solicitors

GNISP, IT consultancy to Oncimmune

HMRC

Journalists, research partners and study sponsors including University of Dundee and University of St Andrews

Third parties to whom we may choose to sell, transfer, or 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.



In relation to Patient Story Data, where you have provided your consent, we may publish the stories and feedback online and through media such as journals, newspapers and magazines. The story may be translated into other languages and be available around the world. Journalists will have some discretion in relation to the nature of their publications subject to industry codes of practice and applicable privacy laws.

We also share data with third parties who provide services to our business where such data is required to enable them to provide the relevant service to us. We do not allow our third-party service providers who act on our behalf 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.

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

In the event that you do not wish to have your personal data disclosed to the third parties listed above you should contact us specifying your particular concerns, which we will consider before responding to you on whether it is lawful and necessary to stop the sharing, on balance.

You may also change your personal preferences to indicate the format, frequency and subject matter of communications you wish to receive from third parties as a result of this disclosure. Please note that this may prevent us from performing the contract entered into with you and we will notify you if this is the case.

6. INTERNATIONAL TRANSFERS

We have commercial relationships with third parties based outside the European Economic Area (**EEA**) which may from time to time entail their processing of your personal data, which may involve accessing or a transfer of person data outside the EEA.

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:

We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission and/or other competent bodies under local laws.

Where we use certain service providers, we may use specific contracts approved by the European Commission and/or other competent bodies which give similar rights over, and protection in respect of, personal data to those within Europe.

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 certify and provide similar protection to personal data shared between the Europe and the US.

Where personal data is published for journalistic purposes the rules in relation to international transfers of data differ, provided certain industry codes and the release is consistent with special journalistic purposes within the public interest.

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

We may share your personal data with the following third parties based outside of the EEA:

Service providers acting as processors who provide IT and system administration services.

Professional advisers including lawyers, bankers, auditors and insurers.

7. 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.



8. DATA RETENTION

How long will you use my 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, accounting, 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 and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for up to 7 years after they cease being customers for tax purposes. Please do not hesitate to contact our Data Privacy Manager if you have further queries in relation to our data retention periods.

In some circumstances we may 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.

9. YOUR LEGAL RIGHTS

Under data protection laws, in certain circumstances, you have the right to:

Request access to your personal data (known as a “data subject access request”). This right 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 any incomplete or inaccurate personal data that we hold about you. We may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. You may 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, 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 where we are relying on a legitimate interest (or those of a third party) and you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms. You also have an unqualified right to object where we are processing your personal data for direct marketing purposes.

Request restriction of processing of your personal data. You may ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) 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 (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer or porting of your personal data to you or to a third party. We will provide 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.

Withdraw consent at any time where we are relying on consent to process your personal data. 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.

If you wish to exercise any of the rights set out above, please contact our Data Privacy Manager.

If you are unhappy with the way in which your personal data has been processed 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 using the contact details above so that your concerns may be dealt with via our internal complaints procedure.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of your legal rights). We may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

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, or otherwise processed inconsistently with your wishes and rights. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests without undue delay and within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.