

PRIVACY POLICY

1. What information does this Privacy Policy provide?

This policy explains how Personal Data is processed for users of a mobile app interface (“**Program**”), designed for patients undergoing treatment for urothelial cancer. The Program features include support information and learning, as well as optional functionalities such as input of the User’s symptoms and mood journal, or for appointment and medication reminders.

“**User(s)**” whose Personal Data may be processed within the Program include:

- Patient Users of the medical condition(s) described above; and
- proxy Users (“**Helpers**”) authorized by a patient to use the Program on their behalf, including caregivers, family members or legal guardians.

If you are registering to use the Program as a Helper, you confirm to have the relevant consent to do so from the patient in question.

The Program:

- has been commissioned by Ares Trading S.A, domiciled at Zone Industrielle de L'Ouriettaz, 1170 Aubonne, Switzerland (“**ATSA**” or “**we**”), an affiliate of Merck KGaA, Frankfurter Strasse 250, 64293, Darmstadt, Germany (“**Merck KGaA (Germany) Group**”); and
- will be provided by Huma Therapeutics Limited, domiciled at 13th Floor, Millbank Tower, 21 - 24 Millbank, SW1 4QP, London (United Kingdom) (“**Huma**”), made available on behalf of ATSA as a bespoke feature on their own application platform (the “**Platform**”).

2. Compliance and roles under Applicable Privacy Law

For the purposes of this Privacy Policy:

- ATSA acts as the *data controller* in determining the essential purposes and means by which Personal Data is processed within the Program.
- Huma acts as a *data processor* in processing such Personal Data on ATSA’s behalf and instructions and as strictly needed to make the Program available to Users.
- “**Applicable Privacy Law**” means any privacy law applicable to your use of the Platform and Program, including the General Data Protection Regulation (EU Reg 2016/679 “**GDPR**”) as a standard reference.
- “**Personal Data**” is typically defined in Applicable Privacy Law as any information capable of identifying an individual either directly (i.e., name, email, address) or indirectly (medical condition, IP address etc.).

We rely on your express consent as the legal basis for processing your Personal Data (including sensitive medical or health information) as a User of the Program, as evidenced by your express acceptance of this Privacy Policy (i.e., GDPR Article 9 (2) (a)). You may withdraw your consent at any time. As per the below, we may also rely on our legitimate interests (i.e., GDPR Article 6 (1) (f)) to develop and improve the Program, typically using such relevant information only in aggregated or high-level form.

3. What Personal Data is processed when using the Program?

a) Profile and Set Up

Access to the Program is enabled via the link provided on the introductory leaflet or alternatively by first downloading the Platform onto a mobile device (i.e. from Google Play, App Store) and then following the relevant instructions on the leaflet.

Creating a profile requires basic account information including name, email address and password, as well as telephone number for security purposes (i.e., where a security code is sent for enhanced verification).

To confirm any requested secondary access, the name, phone number and email address of the Helper is needed to help ensure access entitlement.

b) Within the Program

The following are examples of information that may be requested to adapt the Program to your User profile. Confirming some of these in the Program may be optional.

- Date of birth
- Sex
- Ethnicity
- Language and country of location
- Educational level
- Whether you live alone or with others
- Distance from treating healthcare center.

c) Sensitive health information

The following are examples of sensitive medical or health information that may be requested, provided and processed when using the Program.

- Relevant medical condition and treatment information such as medication dosage, adherence and treatment schedules, or tracking and reminders for medication or appointments.
- Any supporting clinical documentation (such as medical results or a clinical diagnosis) spontaneously uploaded by Users of the Program.
- Adding symptoms or mood in the Program journal feature, allowing patients to follow trends in their symptoms and mood over different points in time, such as information on weight, blood pressure and temperature, nausea and headaches, pain, or fatigue levels and perceived symptom burden.
- Where a User voluntarily chooses to import or synchronize movement data from an external device to allow for the number of steps from GPS data to be recorded and charted over time.

d) Other

Some User Personal Data may be processed for more general or technical purposes, including account configuration, resolving technical issues, debugging and for other standard maintenance and operational activities.

Depending on the settings of the mobile device used by which you access the Program, your thumbprint or personal mobile code may be requested by your device's operating system for security purposes, but this is not directly processed nor accessible by the provider of the Program itself.

4. Who may access or process User Personal Data?

(i) ATSA and companies of the Merck KGaA Darmstadt Group

As the commissioner of the Program, ATSA may receive aggregated information on usage or user engagement ("**Technical Information**") for insight and development purposes. Such Technical Information is typically high-level and is not generally able to identify specific individual Users. The following are provided as examples.

- Usage Analytics: Providing insights on User satisfaction, experience, and suggestions for improvement. Tools may also be used to generate aggregate or statistical insights, such as how many Users are using a specific feature or content item.

The legal basis for this is our legitimate interests in improving and developing the Program, resolving issues some Users may be encountering, and assessing technical capabilities. As an example, the types of mobile device being used, IP addresses and general User locations (i.e., country) can help identify specific accessibility or functionality issues for some Users.

Neither ATSA nor any entity of the Merck KGaA (Germany) Group will be able to view or access information identifiable to specific User accounts, and appropriate technical and operational measures have been taken to ensure that Huma has no general access to view and track User-specific information (see below). Insights on features such as symptoms journals will be strictly limited to general usage insights (i.e. aggregate number of Users regularly using a specific feature).

- User Insights: This could include aggregated User information such as age ranges, locations and genders of Users and will again not generally be identifiable to specific individual Users.

Such information may also be made available as reports or insight analysis within the associated companies of the Merck KGaA (Germany) Group, as well as to our trusted service providers.

(ii) Huma and service providers

Huma, as the Platform provider, is the primary processor of Personal Data from the Program, as well as any sub-processors or service providers it engages (i.e., hosting or storage providers or providers of User support features).

In some cases, some options or features within the Program may result in a User being momentarily redirected to an external page for a limited functional purpose, such as when moving to a different program version facilitated by a subprocess or service provider of Huma. In such cases, a User will be informed if a specific option will result in being directed outside the Program and that some additional processing may occur in executing the command or function, as strictly needed for the purposes of providing the function only (i.e., meta data for purposes of a QR code scan and transition, or using basic identifiers such as email address when changing to a different app version). Some service providers may provide additional information on how they generally process personal data as part of their specific services. You are also free to reduce any processing by service providers by applying the most restrictive settings available in your device's service settings or by any cookie preferences offered by an external site as above.. Please note that in generally hosting the Platform, Huma is not actively screening or viewing information provided by Users or the contents of individual User accounts. Any access to User specific content shall only be to provide

related and requested technical support (i.e., solely as needed to verify and reactivate an account that has been locked).

Further, Huma may view or access any specific User support queries. As such, Users should only provide Personal Data to the extent reasonably necessary for a support query to be successfully handled and/or where specifically requested. Such requests should not generally include any sensitive medical or health information. However, please note, if any information on an adverse event to prescribed medication is inadvertently provided by a User in making a technical support request, Huma will be obliged to report this to the Marketing Authorisation Holder under statutory pharmacovigilance reporting requirements. Such reporting will be strictly limited to the information provided by the User.

(iii) Helper

Helpers using the Program on behalf of a patient will have secondary access to the Personal Data associated to a specific patient's profile.

5. Where is Personal Data processed and how is it protected?

Where Personal Data of Users is physically processed may depend on User location.

For example, the main provider(s) of the Program infrastructure and associated hosting servers are located in the regions cited as follows.

- EU, UK and Switzerland: Within the European Union.
- United States: Within the United States.
- Japan: Japan.

Other Personal Data may be processed by service providers in other locations, such as those providing analytics or usage insights, help and support services, or SMS notification services. Where we transfer your data to a jurisdiction that is not deemed adequate under Applicable Privacy Law, we will ensure appropriate safeguards are put in place. You may request additional information in relation to international transfers of personal data and obtain a copy of the adequate safeguard put in place by exercising your associated rights as set out in Section 8 below.

We will ensure that any processing of Personal Data is compliant with Applicable Privacy Law and securely protected. Relevant operational and technical measures include privacy by design features such as strict role-based access rules, the encryption of Personal Data within the Huma hosting network, pseudonymised User profiles, and suitable documentation and training. We ensure our procedures and security measures are closely monitored and updated where necessary.

Note that the transmission of Personal Data over external networks (mobile phone network provider, or internet service providers) is beyond our reasonable control. Neither ATSA nor Huma can be held liable for any delay, failure, performance, non-performance, or corruption of any information transmitted through external networks.

6. Push notifications

These messages may be sent from the Program to your mobile device, such as for security or notification purposes. Some, such as appointment or treatment reminders, must be expressly activated and can be disabled at any time in your mobile device settings.

7. How long is your data retained for?

Your Personal Data will only be processed for as long as you use the Program, and to help enhance User privacy controls, will be anonymised or deleted after reasonable notice to non-active Users. If you first delete the Platform or Program on your mobile device, your Personal Data may eventually be anonymised in the same way. You may also request Huma to deactivate and anonymise your profile directly as per your rights below.

8. Your associated rights

Your usage of the Program is entirely voluntary and independent from your treatment. You are also free to stop using it at any time. Depending on your location, you may also benefit from some of the following rights under Applicable Privacy Law.

- Right of access: The right to obtain further information on the processing of any Personal Data and to receive a copy of such data.
- Right to rectification: The right to request that any inadequate, incomplete or inaccurate Personal Data is corrected.
- Right to erasure: The right to request for Personal Data to be deleted or anonymised.
- Right to stop processing: The right under certain conditions to stop or restrict the processing of such Personal Data, except where legally permissible or necessary.
- Right to data portability: The right to receive a copy of a User's Personal Data in a structured, common and machine-readable format and/or that such data is transferred to another data controller (where reasonably feasible).
- Right to lodge a complaint with a supervisory authority: The right to raise issues or concern that Personal Data has been processed contrary to Applicable Law, address to the relevant data privacy regulator in your location.

NOTE: If you are participating in a clinical study, specific consent and related terms may also continue to apply. Please contact your specific trial doctor if you have any questions on this.

9. Contact

You may exercise any of your associated privacy rights by writing to Huma's Data Protection Officer, either at the address below or via the email link provided on their company website, currently available at <https://www.huma.com/>.

Huma Therapeutics Limited, domiciled at 13th Floor, Millbank Tower, 21 - 24 Millbank, SW1 4QP, London

If you have any more general questions or concerns on how Personal Data is processed within the Program, you may also address the Group Privacy Officer of the Merck KGaA (Germany) Group either in writing to the address below, by email directly sent to privacy@merckgroup.com or through the data subject request tool available on our company websites such as: <https://www.merckgroup.com/en/privacy-statement.html>.

Merck KGaA, Frankfurter Strasse 250, 64293, Darmstadt, Germany

Please note that for queries on specific aspects of a usage account, some limited Personal Data may be needed or requested for authentication purposes.

Last update: April 2024