|  |  |
| --- | --- |
| **Global Career Privacy Notice** | **Logo  Description automatically generated with low confidence** |

**Who we are**

Hikma is committed to protecting and respecting your privacy. In this notice, when we refer to “**Hikma**”, “**we**”, “**our**” or “**us**” we mean the local Hikma group company or companies to which you are applying or corresponding with, Hikma Pharmaceuticals LLC and Hikma Pharmaceuticals USA Inc. When we say "**Hikma Group**" we are referring to all Hikma group companies.

**Websites covered by this privacy notice**

This Global Career Privacy Notice (the “**Privacy Notice**”) sets out the basis on which we will use any personal data that we collect about you in connection with Hikma’s recruitment and onboarding processes and should be read in conjunction with our website privacy policy (which can be found on our website **https://www.hikma.com/privacy-policy/.**) (the “**Website Privacy Policy**”). Our Website Privacy Policy contains information about the cookies that we use on our website.

In brief, this Privacy Notice explains:

* what personal information we hold and why we process it;
* the legal grounds that allow us to process your personal information;
* where the data comes from, who has access to the data and how long we keep it; and
* how to contact us concerning your data.

Please read this Privacy Notice carefully to ensure that you understand how your personal data will be used by Hikma during the recruitment and onboarding process. Hikma will regularly review this Privacy notice and may amend it from time to time. Any changes will become effective when we post the revised Privacy Notice on our careers website and we will notify you of any significant changes where we are required to do so.

Our careers website may contain links to websites or applications which we do not control and to which this Privacy Notice does not apply. Please ensure you read the privacy notices on those websites to know more about the personal data collected by these third parties and how it is processed.

**How we collect your personal data**

You may provide your personal data when you create an account to access and use our careers website, apply for a role listed on our careers website, contact us regarding a career opportunity, share your CV or resume on the careers website or through other means, or take part in an interview or selection process.

Hikma may also obtain information about you from other sources, including third party recruiters, agents, previous employers, referees, educational institutions attended by you, or third parties providing services which allow us to verify the details that you provide to us (for example, when we undertake criminal records or identification checks), if permitted by applicable law.

If you are successful as part of the recruitment process, and in accordance with this Privacy Notice, we may undertake a more detailed pre-employment screening or background check as part of the onboarding process as set out in the section below. If you have concerns about this, you should speak to your HR contact within the Hikma entity recruiting you for the position.

**Why we collect your personal data**

The type of personal data that we request from you and the way we use that data will vary and are determined by the requirements of the country that the role you apply or enquire for is located, and applicable laws. The table below sets out in more detail the type of personal data we use and why.

| **Purpose for which we use your personal data** | **What type of personal data do we use?** | **What lawful basis do we rely on to use your personal data?** |
| --- | --- | --- |
| To create your account on the career website | * Email address, password, first name, last name, country of residence. * Account settings regarding accessibility of your profile, your willingness to receive new job posting notifications and information about career opportunities. | Legitimate interests: it is in our legitimate interest in managing our recruitment process (we will not rely on this ground if our legitimate interest is overridden by your interests or fundamental rights and freedoms). |
| As part of the recruitment process to communicate with you, assess your suitability for the position you are applying for and arrange and conduct interviews or other assessments or pre-employment tests. | * Profile Information (including first name, last name, email, phone, address, city, country, state/province/region, travel preference, highest education level, education and work experience information, resume, cover letter, language skills, accounts settings and professional certifications). * Other Application Specific Information (e.g right to work information, work authorisation). * Evidence of qualifications, references, results of assessments and interview notes. * If you contact us in relation to your application, record of our correspondence. | Legitimate interests: it is in our legitimate interest in conducting the recruitment process (we will not rely on this ground if our legitimate interest is overridden by your interests or fundamental rights and freedoms). |
| As part of the onboarding process:   * to prepare your offer of employment and any other documents and tests and training activity required in connection with your contract of employment; and * to manage the terms and conditions of your employment, such as payment of wages/salary, direct deposit authorization, the provision and administration of benefits and leaves of absence and maintenance of emergency contact information. | * Identity information, such as name, date of birth and information regarding your identify documents (such as passport information). * Contact information, such as your home address, email address and telephone number. * Financial information such as your salary, company allowances, bonus, benefits, taxpayer reference number and bank account details. * To the extent permitted by applicable laws, we may also use your information to conduct checks and verify the details that you provided to us. This may include the processing of special category data obtained from criminal background checks. * To the extent permitted by applicable laws race and ethnicity information (optional information). * To the extent required to perform your employment contract in certain countries in the Middle East and North Africa region, your religion. | * Contractual: it is necessary prior to entering into a contract with you or in order to perform an employment contract; and/or * Legal obligation: it is necessary to comply with laws and regulations. |
| If you have asked us to keep you informed of other opportunities in the Hikma Group, to include you in our global talent pool, consider you for opportunities in any of the companies which are part of the Hikma Group and contact you about those opportunities. Members of the Hikma Group may do this in various ways, including through the career website or by e-mail. | Profile Information (including first name, last name, email, phone, address, city, country, state/province/region, travel preference, highest education level, education and work experience information, resume, cover letter, language skills and professional certifications and settings regarding accessibility of your profile). | Consent: you have consented to the processing. |
| If you have created job alerts on your profile, to send you the alerts you requested. | Profile Information (including full name, email and alert preferences). | Consent: you have consented to the processing. |
| In countries where it is permitted by law, to promote and monitor equal opportunities within the Hikma Group. | Religious or similar beliefs, ethnic origins and veteran status. | * Contractual: it is necessary prior to entering into a contract with you or in order to perform an employment contract; and/or * Legal obligation: it is necessary to comply with laws and regulations. |

In addition to the above, we may use your information:

* to comply with applicable laws, regulations and professional obligations;
* to prepare and maintain legally required records, such as I-9 forms, W-4 forms, 1099 forms, EEO-1 forms, and affirmative action plans in the U.S;
* to protect against fraud or other illegal activity or for risk management purposes;
* to establish, exercise or defend our rights and/or rights of our employees or a third party;
* to achieve other operational purposes for which the personal information was collected that are compatible with the context in which the personal information was collected and our employment or independent contractor relationship;
* to respond to any of your queries or to any request from competent authorities; and/or
* to ask you to update your profile or tell you about changes to our policies or applicable terms.

We will not use your information for any other purpose, unless we have a legal right or obligation to do so.

We will notify you when we ask for the information, whether providing certain information is optional or necessary (pursuant to a statutory or contractual obligations or otherwise), in order to assess and consider your application.

**Special Category or Data and Protected Classification Information**

Special category data includes information around race and ethnicity, health, trade union membership, philosophical beliefs, sexual orientation, and other categories as prescribed by law.

In the U.S., protected classification information includes characteristics of protected classifications under U.S. federal or California law, such as (race, color, national origin, religion, gender (including pregnancy), disability, age (for individuals aged 40 years old and above), citizenship status, sexual orientation, gender identity and gender expression).

As set out in the above section, in some countries, we may collect special category data or protected classification information about a candidate as part of the recruitment and/or onboarding process to the extent that we are required to do so to comply with applicable laws. You can decide whether to give us special categories of information or protected classification information, if we ask you for them. Not providing such information will not affect your application and if you provide us with this information it will not be considered in the recruitment or selection process.

When completing your application, we would prefer that you avoid submitting the following sensitive information, except where such information is legally required or needed for us to comply with our legal obligations and internal policies relating to diversity and anti-discrimination: medical or health conditions, family medical history, or genetic information

**Automated Decision Making**

We do not currently use any automatic decision making as part of our recruitment processes, although we may use filtering questions in order to assist us with the administration and progression of your application throughout some stages of the application process.

**How long do we keep your information?**

We will only retain the personal data that you provide in connection with the purposes set out in this Privacy Notice for as long as it is necessary in order to achieve these purposes.

We will delete your account if you have not logged into your account within two years from the last activity.

We will retain your information in relation to a specific application or onboarding process for as long as necessary to achieve the purposes for which it was collected or processed or as it is established in the applicable laws related to data retention periods or as permitted by applicable laws. The period for which we store your personal data collected during the recruitment and onboarding process will vary depending on the type of personal data, the role or opportunity you are applying for, how the personal data is used, and applicable laws and regulations. If you would like more information about Hikma’s retention periods for recruitment and onboarding activities, please contact us at privacypolicy@hikma.com.

If you become employed by us we will keep your personal information for the duration of your employment and for a period afterwards as set out in the relevant Hikma employee handbook.

**The conditions under which we can share it with others**

Your personal data may be shared with third parties to the extent necessary to comply with laws and regulations or to support the detection, investigation and prevention of criminal activities.

The global nature of our business means that your personal data may be shared within the Hikma Group. This will involve your data being transferred to and stored in countries outside the United Kingdom (“**UK**”) and the European Economic Area (“**EEA**”) (including Jordan and the USA) which may not have the same level of data protection as your home country. It may also be processed by staff operating outside the UK and the EEA who work for us and need to see your personal data to help us with the administration or our recruitment and onboarding process. We put in place appropriate measure (such as model contractual clauses), in line with any applicable legal requirements, to adequately protect your personal data.

Your personal data may also be shared with third parties who provide services to us as part of the recruitment and onboarding process including recruitment agencies, consultants, background services providers, professional advisers, survey providers, cloud services providers and other technology providers who assist us in developing and improving the careers website. These third party providers may process your personal data outside of the UK or the EEA. To the extent applicable, when transferring personal data outside the UK or the EEA, we will put in place appropriate measure (such as model contractual clauses), in line with any applicable legal requirements, to adequately protect your personal data or ensure that the country in which your personal data will be processed has been deemed “adequate” by the European Commission.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to us; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

**How we keep your personal data secure**

We have appropriate security policies in place which are intended to ensure, as far as possible, the security and integrity of all our information, including your personal information.

The service providers we work with are carefully selected and we check they have adequate security measures and technologies in place to protect your personal information.

**Your personal data rights and how to exercise them**

In the UK and the EEA and some other countries you may have certain rights available to you to exercise control over your personal data under applicable data protection laws. These rights include the right to request access to any of your personal information which we may hold,  the right to ask us to correct any mistakes in your information, to delete your personal data, or to provide you with a copy of your personal data to be used for your own purposes, by sending an e-mail to privacypolicy@hikma.com.

You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data by us and we can be required to no longer process your personal data. If you have a right to object and you exercise this right, your personal data will no longer be processed for such purposes by us.

Please note that those rights do not always apply and there are certain exceptions to them depending on our reason for processing your personal information and the local law in your jurisdiction. We may also need to confirm your identity before responding and acting on your request.

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. Alternatively, we may refuse to comply with your request in these circumstances.

**Information about Hikma**

For the purpose of the General Data Protection Regulation (EU 2016/679) and the UK GDPR,the data controller is the Hikma recruiting entity, Hikma Pharmaceuticals LLC and Hikma Pharmaceuticals USA Inc. UK GDPR means the General Data Protection Regulation (EU) 2016/679 in such form as incorporated into the law of England and Wales, Scotland and Northern Ireland by virtue of the European Union (Withdrawal) Act 2018 and any regulations thereunder.

**Data Privacy Contact Details and Complaints**

If you have any feedback or questions on this Privacy Notice, or wish to exercise any of your rights, please send an e-mail to privacypolicy@hikma.com. For applicants in the UK and the EEA, you also have the right, if necessary, to lodge a complaint regarding the use of your personal data with your country’s data protection or applicable supervisory authority. In the UK, the Information Commissioner’s Office is responsible for data regulation, and can be contacted via +44 (0) 303 123 1113. If we cannot resolve your questions or concerns, you also have the right to seek judicial remedy before a national court.