

On 25th May 2018, the General Data Protection Regulation (GDPR) comes into force giving individuals in the European Union enhanced rights over the use of their personal data. As a result, we have updated our privacy policy to give you transparency about how we collect, use and keep your data safe, and what your rights are under the GDPR.

Who is InnerCircle?

InnerCircle is a healthcare communications agency and a 'data controller' in respect of the data that it collects and stores. There are two types of data under GDPR:

- **Personal data** (that can be used to identify you directly or indirectly): Such as name, job title, contact details, bank details, passport details, date of birth, etc
- **Sensitive personal data** (that could be used in a discriminatory way to profile you): Such as religious beliefs and opinions, sexual orientation, biometric data, physical and mental health conditions, ethnicity, etc

1. What personal data information do we collect?

Our collection of personal data is limited and proportionate to its legitimate purpose which is business-related only. We collect **personal data** about you, including:

- Name, job title, organisation
- Contact information including email and phone number

2. What sensitive personal data information do we collect?

In some cases, we also collect **sensitive personal data** about your health. We only do this if (a) you have subscribed to receive information through a patient support programme we are delivering on behalf of our client, or (b) if you tell us that you have had problems with our pharmaceutical clients' medication or device and we need to manage and report those problems to our client and their pharmaceutical governing bodies.

3. How do we collect it?

We collect personal data about you when you:

- Contact or interact with us directly
- Through third party suppliers
- Visit our website
- Engage with us on social media i.e. LinkedIn and Twitter

4. What do we do with this personal data?

We require this data to supply services to our clients and to provide you with relevant information that either relates to your role or because you have asked us to send it to you. We also need to keep it in order to comply with our business, legal and regulatory obligations (such as pharmaceutical compliance, HMRC, reporting to pharmaceutical governing bodies, legal processes and laws).

5. Legitimate interest

5.1 If you are a client, or have been a client in the last seven years

We collect, store and handle the personal data of current and historic clients based on legitimate interest. We only collect personal data that we need in order to provide you with information that is relevant to your job or the services we have provided to you. We do not hold any sensitive personal data on current or historic clients.

Our ability to communicate with you serves your interest, as a client, or historic client, who has engaged our services.

We use your data to:

- Provide you with our services
- Comply with our business obligations (such as pharmaceutical compliance, HMRC, Pharmaceutical governing bodies)
- Comply with laws and legal proceedings (for example if we have to respond to court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims)

5.2 If you are a supplier, or have been a supplier in the last seven years

We collect, store and handle the personal data of current and past suppliers based on legitimate interest. We only collect personal data that we need in order to provide you with information that is relevant to your job or the services we have engaged you to provide. We do not hold any sensitive personal data on current or past suppliers.

Our ability to communicate with you serves your interest, as a current or past supplier, whose services we have purchased.

We use your data to:

- Engage with you to request service delivery
- Comply with our business obligations (such as pharmaceutical compliance, HMRC, Pharmaceutical governing bodies)

Last updated: 21/02/2023

- Comply with laws and legal proceedings (for example if we have to respond to court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims)

5.3 If you are a journalist, blogger or Patient Advisory Group

We collect, store and handle the personal data of journalists, bloggers and Patient Advisory Groups based on legitimate interest. We only collect personal data that we need in order to provide you with information that is relevant to your job. We do not hold any sensitive personal data.

Our ability to communicate with you serves your interests, as a journalist, blogger, or Patient Advisory Group who writes about or would benefit from receiving information about the clients that we represent. It means we can keep you informed of our clients' news via telephone, emails and mailings. It also serves the interests of our clients, who want to share relevant information with you.

We use your data to:

- Tell you about a news story or share our ideas for a feature
- Send you invitations to events
- Call you, or return your calls to us
- Introduce a spokesperson
- Gauge your interest in supporting a campaign/programme

5.4 If you are a healthcare professional

We collect, store and handle the personal data of healthcare professionals based on legitimate interest. We only collect personal data that we need in order to provide you with information that is directly relevant to you. We do not hold any sensitive personal data on healthcare professionals.

Our ability to communicate with you serves your interests, as a healthcare professional who manages patients with conditions that our clients provide care solutions for. It means we can keep you informed of educational opportunities and events that are relevant to your field via telephone, emails and mailings. It also serves the interests of our clients, who want to share relevant information with you.

We use your data to:

- Provide information on educational opportunities relevant to your field
- Invite you to educational events that are relevant to your field
- Report adverse events (relating to your patients on our clients' medications / devices)

Last updated: 21/02/2023

- Comply with our business obligations (such as pharmaceutical compliance, HMRC, pharmaceutical governing bodies)
- Comply with laws and legal proceedings (for example if we have to respond to court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims)

5.5 If you are a patient

We collect, store and handle the personal data of patients based on legitimate interest. We collect both personal data and sensitive personal data about your health.

We only do this if you tell us that you have had problems with our pharmaceutical clients' medication or devices or if you have subscribed to receive information through a patient support programme we are delivering on behalf of our client. We do this for the purposes of managing and reporting information about side effects or product failures to pharmaceutical governing bodies.

Our ability to communicate with you serves your interests, as a patient who has:

- Subscribed to a patient support programme that we are managing for our pharmaceutical client
- If you, or a relative or healthcare professional, advise us that you have had problems with your medication

We use your data to:

- Manage your subscription to a patient support programme
- Advise our clients and their pharmaceutical governing bodies of any problems you have had with their medications or devices

5.6 If you are enquiring about a job

If you make an enquiry about job opportunities, we will also gather personal information that you provide to us, via your CV and covering letter, which may include: your name, gender, contact details, education/work history, nationality ("Career Information").

Some of the Career Information identified above is classed as sensitive personal information. We will only collect and process sensitive personal data in so far as it is necessary to ensure that we conform with legal requirements for example under equality of opportunity laws and to monitor our success in reaching out to a diverse prospective workforce. In order to fulfil our obligations under the GDPR we require your explicit consent to be able to process sensitive personal data. You will be asked to do this when you submit your Career Information.

6. How long do we keep your data?

Last updated: 21/02/2023

6.1 Personal data: All personal data is deleted after a period of 12 months if there is no legitimate interest or legal basis requiring us to retain it (e.g. HMRC require companies to retain financial information for seven years).

6.2 Sensitive personal data: For legal reasons we need to keep a copy of your sensitive personal data for a longer period:

- If you have subscribed to a patient support programme that we are managing for our client, our policy is to deactivate (rather than delete) your data if you advise us that you want to come off that programme because we are required, by pharmaceutical governing bodies, to hold your data whilst the programme is running and for two years after the patient support programme terminates. At that time, we will then securely destroy your sensitive personal data
- If you, or a relative or healthcare professional, advise us that you have had problems with your medication or device, we are required by law to share this information with the pharmaceutical company and retain the information for seven years
- If you submit career information we retain this for 12-months. If your application is successful it will be retained for the period you work at any of the affiliate companies with the InnerCircle in accordance with our standard employment procedures

7. How do we protect your data privacy?

We are committed to ensuring that your data is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure your data. All the personal data that we handle is processed by our GDPR trained staff in the UK. We have comprehensive internal policies around the storage and management of your data. Your personal data is stored securely on our firewalled server. Your data is also password protected and access is restricted to relevant individuals within InnerCircle.

We have not, and do not, sell data.

For the purposes of IT maintenance, we back-up your data onto servers within the European Union. We do not carry out any automated decision making which is likely to have a legal or similar effect on you. All our staff are aware of our data protection policies.

We take appropriate technical and organisational measures to safeguard the personal data that you provide to us but no transit over the internet can ever be guaranteed so we cannot guarantee the security of any data that you transfer over the internet to us.

8. How we share your personal data and who we share it with

We may share your data with:

Last updated: 21/02/2023

- Relevant clients
- Selected staff members

In addition to sharing your personal data as indicated above, we disclose data under the following circumstances:

- Third-party service providers: to facilitate or to provide certain services on our behalf. This may include:
 - Our IT maintenance company
 - Travel companies (including hotels, airlines, taxi companies) so that we can book travel on your behalf
 - Our relevant client
 - A third-party (if we are jointly working with one on a particular programme)
 - Mailing and database management companies that administer our patient support programmes
- Pharmaceutical companies and pharmaceutical governing bodies, if you, a relative, or a healthcare professional, advises us that you have a problem with your medication or device
- In order to comply with laws and legal proceedings, for example if we have to respond for legal reasons or are required by law to provide supporting data

9. Links to other websites

Our website may contain links to enable you to visit other websites of interest easily. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

10. How we use cookies

Similar to other commercial websites, our Website uses a standard technology called “cookies” and web server logs to collect information about how our Website is being used.

A cookie is a small file which asks permission to be placed on your computer’s hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

Last updated: 21/02/2023

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

We use 'session' cookies which enable you to carry information across pages of the Website and avoid having to re-enter information. Session cookies enable us to compile statistics that help us to understand how the Website is being used and to improve its structure. We also use 'persistent' cookies which remain in the cookies file of your browser for longer and help us to recognise you as a unique visitor to the Website, tailoring the content of certain areas of the Website to offer you content that match your preferred interests. This explains what we use and how it

works: <http://code.google.com/apis/analytics/docs/concepts/gaConceptsCookies.html>

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. Please note that this may prevent you from taking full advantage of the website.

11. Controlling your personal data

Under the GDPR you have more control about the personal data we hold on you. You can restrict the collection or use of your personal data in the following ways:

- You can withdraw your consent to the processing of your personal data
- You can request we delete your personal data
- You can restrict how we process your personal data
- You can ask us what personal data of yours we hold, how we obtained it and how long we intend to keep it
- You can ask us to change your personal data because it is inaccurate or incomplete
- You can let us know if you don't want your personal data shared with a third party

Your rights above can be exercised free of charge by:

- Sending an email to willoughby@innercircle.support; or
- By writing to us at Data Protection Officer, 1 Little Bowden Cottages, Upper Basildon, Reading, RG88JG



Last updated: 21/02/2023

For security purposes, and to comply with GDPR, we will need to satisfy ourselves of your identity before we can action a request to see your data

We are wholly behind the GDPR and the need to give you more control over the data that organisations can hold on you. Unfortunately, please do note that, if by exercising one or more of your rights requires deletion of your file, or restriction on the special personal data we have access to, we may not be able to provide you with some of our clients' services. We also may only be able to deactivate your data (rather than permanently deleting it) if it contains information required to meet our clients', and our own, legal obligations. If we are unable to comply with your request we will let you know what the reason is.

If you feel that any of your rights have been infringed, you have the right to lodge a complaint with the Information Commissioner's Office (www.ico.org.uk).