Privacy Notice

Prepared by: Data protection Correspondent and the DPO

Document ID	2022.06.21_Privacy_Notice_PN_v1.1
Version	1.0
Publication date	21 June 2022
Next review date	21 June 2023
Approved by	DM and DPO

We keep this table

Version	Date of Change	Responsible	Summary of Change
1.0	15 June 2021	DM/DPO	Description of collected categories of data, clarification of legal basis, role of MyC and Customers, procedure for Data subject to exercise their rights.
1.1	21 June 2022	DM/DPO	Add of DataDog to the third parties.
2			
3			

Table des matières

PRIVACY NOTICE

How to use this Privacy Notice

This notice is layered, so you can easily find the information that is applicable to you. Please click the through to the headings or subheadings of the specific areas set out below to read the full text.

There is a Glossary of terms at the end of this document to help you understand the meaning of some of the terms used in this privacy notice.

Introduction – please read me

Please read this Privacy Notice and any other privacy notice or fair processing notice we may provide on specific occasions carefully, as it is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export and delete your information.

This Privacy Notice supplements the other notices and is not intended to override them.

Who we are

MyC is a company incorporated and registered in France with company number 890 755 275, whose registered office is at 113 avenue du Président Salvador Allende, 93100 Montreuil, FRANCE.

MyC is operating in health field and specialized in health data management, for additional information please click here .

This privacy notice is issued on behalf of MyC, when we mention "we", "us" or "our" in this privacy notice, we are referring to MyC responsible for processing your data.

Websites

The following websites and apps are in scope of this privacy notice:

- https://www.myc.doctor/
  https://app-eu.myc.doctor
- https://app.myc.doctor

Controller/Processor

We are registered with the pertinent data protections authorities in line with the applicable legislation. To find out more on our registrations please contact us.

We do not and will not sell your data to third parties.

We act as the Controller regarding personal data necessary for creating and managing a user account as well as personal data related to the use of website and applications this privacy notice refers to.

We act as the Processor for processing activities conducted through our platforms/services purchased and used by Customers, namely for personal data collected by Customers for patient, appointment, consultation and monitoring. While we act as a Processor, we process data according to the instructions received by our Customers (acting as the Controller) who are responsible for dealing with your requests aimed at implementing your data privacy rights. For exercising your rights, you need to contact the pertinent Customer directly.

In some cases, we may act as a Joint Controller together with the Customer. In that case you will be referred to a specific privacy notice explaining the responsibilities of each party and the procedure for you to exercise your rights.

Notwithstanding the role MyC is covering, MyC takes seriously privacy and take all the necessary measures to ensure personal data processing activities are conducted in compliance with the applicable Data Protection Law.

Our commitment to you

We respect your right to privacy and are committed to protecting it and complying with Data Protection Law. We will always keep your Personal Data safe. We will be clear and open with you about why we collect your Personal Data and how we use it. Where you have choices or rights, we will explain them to you and respect your wishes.

How to contact us

If you have questions about this Privacy Notice or the processing of your Personal Data, please contact us at:

Postal address

MyC
113 avenue du Président Salvador Allende
93100 Montreuil
FRANCE

Email

privacy@myc.doctor

Our DPO (outsourced)

We have appointed GRCI Law Limited, to act as our DPO.

Postal address
GRCI Law Limited /IT Governance Europe Ltd
3 rd Floor, Boyne Tower,
Bull Ring, Lagvooren, Drogheda,
Co. Louth, A92 F682, Ireland

Email: dpoaas@grcilaw.com

Tel: +44 (0)333 800 7000

Please ensure you include our company name in any correspondence you send to our DPO.

Personal information we collect about you as a Controller

We process different kinds of Personal Data about you depending on your relationship with us (Costumer, supplier, user):

Identity data

Includes first *name, last name, other names, date of birth, professional registration.*

Contact data

Includes your contact address, billing *address, email address and telephone number(s).*

Location data

We may collect your location data from your IP address and telephone codes.

Transaction data

Includes details about payments to and from you and other details of services you have purchased from us.

Technical data

Includes IP address, your login information, time zone setting and location, browser plugin types and versions, operating system and platform, and other technology on the devices you use to access our website or our Apps

Profile data

Includes your email and password, the services you have used on our website and/*or our Apps*, your use of social media functions on our Website and/ *or our Apps* for *authentication, feedback, survey responses and such information as you provide to us.*

Usage data

Includes information about how you use our Website and *or Apps,* the resources you access, pages you visit, the time and date of your visit or an email opened, the time spent on those pages, unique device identifiers, the URL (Uniform Resource Locator) clickstream to, through and from our website and other diagnostic data.

Chat sessions

This information includes online chat sessions and the chat history of previous sessions.

Special Category Personal Data

Special Category Personal Data is personal data that needs more protection because it is sensitive, and we may collect this type of personal data on the behalf of our Customers in the course of providing our services or during our interactions with you.

Your online chat sessions may contain Special Category Personal Data you have decided to share.

We will not process your Special Category Personal Data and shall we be in such situation will be not processing Special Category Personal Data without a Lawful Basis to do so.
.

How we get your Personal Data

We use different methods to collect data from and about you through our websites, by telephone, through LiveChat and through any related social media applications, including:

Personal Data provided directly by you

You may give us your Personal Data by filling in forms, surveys, questionnaires or assessments on our Website, or by corresponding with us by post, phone, email, chat or otherwise. This includes Personal Data you provide when you:

- Register to use our *Apps,* Website or services, or to receive general information on our services.

Data we collect when you use our Websites and Apps

Each time you interact with our Website, we will automatically collect Personal Data, including technical data about your device, your browsing actions and patterns, content and usage data. We collect this data using Cookies, server logs and other similar technologies like pixels, tags and other identifiers in order to remember your preferences, to understand how our Website and Apps are used.

Please see our Cookie Notice here for further details.

Information we receive from third parties

We may receive Personal Data about you from various third parties, such as:

a) Device data from the following parties:
   - Analytics providers such as Google.
   - Advertising networks.
   - Search information providers.

b) Technical data and device data from the following parties:
   - Analytics providers such as Google
   - Advertising networks such as Google.

c) Providers collecting survey information;
d) Information about our candidates from referees, recruitment agencies and social media such as LinkedIn; and
e) Reviews from providers.

Unique application numbers

When you want to install or uninstall a service containing a unique application number or when such a service searches for automatic updates, that number and information about your installation, for example the type of operating system, may be sent to us.

How we use personal information

General

We need your Personal Data to conduct our business and provide you with *our Apps and* services. Most commonly we will use your Personal Data in the following circumstances:

- Where you have consented before the processing.
- Where we need to perform a contract, we are about to enter or have entered 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.

UK GDPR/EU GDPR Lawful Basis table

The table below describes the ways we use your Personal Data, and which Lawful Basis we rely on to do so. We have also identified what our legitimate interests are where appropriate.

For more information on the Lawful Basis we use to process your data under the UK GDPR and EU GDPR, see our Lawful Basis table below or contact us.

Lawful Basis Table

LAWFUL BASIS	PURPOSE EXAMPLES
Contractual obligations We use your Personal Data on the basis that it is necessary for us to provide our services and products to you. When you purchase a service and/or use our *Apps and* Website or register with us, you are entering into a contract with us.	**Onboarding** When you register as a new client, supplier, user. We may use your personal, contact, technical, profile and communication data. **Service delivery** In order to be able to deliver our services or receive services in physical or digital form. To provide you with information, products or services that you requested from MyC and to notify you about changes to our service. The fulfilment and distribution of physical or digital products to our users. When we manage and store your chat sessions. **Account administration** ● When we administer accounts, take, or receive payment, deal with any transaction, respond to queries, refund requests and complaints. ● When we collect and recover money owed to us We use *Identity Data, Contact Data, Transaction Data* to administer accounts. **Relationship management** To manage our relationship with you, which may include: ● Notifying you of changes to our terms or Privacy Notice; ● Notifying you of changes to *the Apps or* any services processing and delivering your services and incentives. ● Processing orders; and ● Asking you to leave a review or take a survey. We use *Identity Data, Other Identifiers, Contact Data, Location Data, Transaction Data, Profile Data, Chat Sessions* to manage our relationship with you. **Communication** To be able to contact you regarding updates or informative communications related to the functionalities, products, or contracted services,

	including security updates, when necessary or reasonable for their implementation. Handling the information, you submit to us enables us to respond effectively. We may also keep a record of these queries to inform any future communications between us and to demonstrate how we communicated with you throughout our contractual relationship. We use Identity *Data, Contact Data, Transaction Data, Profile Data and Chat Sessions to* help us to communicate with you.
Legitimate interest When we rely on this, we will carry out a Legitimate Interests Assessment to ensure we consider and balance any potential impact on you (both positive and negative), and your rights under Data Protection Law. Our legitimate business interests do not automatically override your interests – we will not use your Personal Data for activities where our interests are overridden by the impact on you unless we have your consent or are otherwise required or permitted to by law.	**Managing our business** We hold Personal Data for our own legitimate business interest. This relates to us managing our business to enable us securely to provide our services/products: ● When we respond to your queries and complaints, where you are not a user, client or supplier, or a potential client, user or supplier. ● When we carry out our obligations arising from any contracts entered into between you and MyC. ● When we monitor trends so we can improve our services and Website *and Apps*. and in the context of a business reorganisation or group restructuring exercise. We may use your personal, contact, technical, profile data. It is necessary to process this personal data 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. **Provide and maintain Websites and Apps.** It is in our legitimate interests to process personal data for our legitimate interests for running our business, provision of administration and IT services, network security and ● to prevent fraud. ● to provide and maintain our Websites, Apps and platforms, including to monitor the usage of these, troubleshooting, data analysis and system testing necessary for our legitimate interests (for running our business, provision

of administration and IT services, network security) an do limit our business, cyber and legal risk.

- to ensure that our website content is presented in the most effective manner to clients, which is in our legitimate interest to keep users and clients engaged in our website and services to help towards the growth of our business.

The personal data we use to provide and maintain Websites and Apps includes *Identity Data, Other Identifiers, Contact Data, Location Data, Technical Data, Transaction Data, Profile Data, Chat Sessions, and Usage Data.*

Recommendations and marketing to Customers

It is in our legitimate interests to use marketing to grow our business and ensure commercial viability by marketing to Customers and we use personal data to:

- make recommendations to Customers about services that may interest you.

- To make suggestions and recommendations to Customers about goods or services that may be of interest and necessary for our legitimate interests (to develop our products/services and grow our business).

We may use personal data from existing clients for these purposes and this data includes *Identity Data, Contact Data, Technical Data, Transaction Data, Profile Data and data collected from Chat Sessions.*

Security

It is in our legitimate interests to process personal data securely to maintain network security and:

- to prevent fraud when users are transacting on our Website,
- to ensure our Websites and systems are secure.]to prevent financial and reputational loss to our business.

Recruitment of candidates (contractors, employees and providers)

	We will use the personal information we collect about you to assess your skills, qualifications and suitability for the work. It is in our legitimate interests to decide whether to appoint you to work with us since it would be beneficial to our business to appoint someone with the correct qualifications and experience to be able to do their job efficiently and beneficially to our company. We use *Identity Data, Contact Data, Location Data and Candidate Data to* assess your suitability for a position and to communicate with candidates. **Reviews** When we capture your service reviews, for example when you buy goods and services from us, we may follow it up with an enquiry about your experience of the service to help us gauge Customer satisfaction. It is in our legitimate interests to ensure our survival in a competitive market by ensuring that our services and goods are market appropriate and delivered satisfactorily to our clients and users. We use *Identity Data, Contact Data, Transaction Data, Chat Sessions to* be able to properly communicate and respond to reviews. **Research and analysis** For statistical analysis, so that we can monitor and improve services, Websites and Apps, or develop new ones. It is necessary to us and in our legitimate interests (to study how Customers use our products/services, to develop them, to grow our business). We use *Identity Data, Other Identifiers, Contact Data, Location Data, Loyalty Data, Technical Data, Profile Data, Candidate Data, Chat Sessions, Usage Data* for research and statistical analysis the type of personal data we use depends on the nature of the research and analysis. **Data analytics** We use data analytics to improve our Website, products/services, Customer relationships and experiences. Data Analytics are necessary to our business and in our legitimate interests to define types of Customers for our products and services, to study how Customers use our products/services so we are able to develop

	our products and services and keep our website and services updated and relevant. We may use *Location Data, Technical Data, Profile Data, Chat Sessions and Usage Data for data analytics.* **Rights and claims** It is in our legitimate interests to use personal data, where it is necessary, ● to enforce or apply our Website terms of use, our policy terms and conditions, or other contracts. ● to exercise our rights, to defend ourselves from claims and to keep to laws and regulations that apply to us and the third parties we work with. Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud, We may use *Identity Data, Other Identifiers, Contact Data, Location Data, Technical Data, Profile Data, Candidate Data, Chat Sessions, Usage Data for* these purposes.
Legal obligations We may use your Personal Data to comply with laws (for example, if we are required to co-operate with a police investigation after a court order orders us to).	**Legal requirement** The processing is necessary for compliance with our legal obligations, such as but not limited to healthcare requirements, security requirements and accounting requirements. To comply with applicable law, for example in response to a request from a court or regulatory body, where such request is made in accordance with the law. We may use *Identity Data, Other Identifiers, Contact Data, Location Data, Technical Data, Profile Data, Candidate Data, Chat Sessions, Usage Data for* these purposes. **Data subject rights** Verifying your identity when you exercise your data subject rights. Fulfilling data subject rights requests. We may use *Identity Data, Other Identifiers, Contact Data, Location Data, Technical Data, Profile Data, Candidate Data, Chat Sessions, Usage Data for* these purposes, dependent on the Data Subject request itself.

	Criminal activity To detect fraudulent or criminal activity, we may share information with forces such as the police. We may use *Identity Data, Other Identifiers, Contact Data, Location Data, Technical Data, Profile Data, Candidate Data, Chat Sessions, Usage Data for* these purposes.
Consent We may have to get your consent to use your Personal Data, this could be necessary if we need to process Special Category Personal Data about you or when we use cookies. You have the right to withdraw consent at any time by contacting us. Wherever consent is the only reason for using your Personal Data, you have the right to change your mind and/or withdraw your consent at any time by clicking the Unsubscribe button at the bottom of an applicable email or by withdrawing your consent here.	**Cookies** ● To monitor trends so we can improve the Apps. ● To facilitate visitors' use of the Websites, we may collect IP addresses and store Cookies on visitors' devices. We may use *Identity Data, Contact Data, Location Data, Technical Data, Chat Sessions, for* these purposes. **Installation** To install an App and register you as a new App user. We may use *Identity Data, Contact Data, Location Data, Technical Data, Chat Sessions and Usage Data for* these purposes. **Location** When you use our *Apps or* use our website, you may allow us to obtain your precise location from your device. We use this information to deliver personalised content and for analytics. We may use *Location Data, Technical Data, and Usage Data for* these purposes.

Special Category Personal Data

Reason for processing Special Category Personal Data:

We will be not processing Special Category of Data unless this is required by our Customers.

Shall we be processing Special Category Personal Data, you will be duly informed and we must, in addition to the Lawful Basis in the Lawful Basis table, process your Special Category Personal Data because of an additional condition, including the followings :

- You have given us your explicit consent to process that data.

- We are required by law to process that data in order to ensure we meet our 'know your client' and 'anti-money laundering' obligations (or other legal obligations imposed on us).
- The processing is necessary to carry out our obligations under employment, social security, or social protection law.
- The processing is necessary for the establishment, exercise, or defence of legal claims.
- You have made the data manifestly public; or
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes.

For more information about us using your Special Category Personal Data, please contact us.

Using your data for other reasons

We will only use your personal information 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 information for an unrelated purpose, we will notify you and we will explain the Lawful Basis that allows us to do so.

Marketing and advertising

Using Personal Data for marketing purposes

We currently do not use data for marketing purpose. We may use information of Customers to provide details about services.

Shall we in the future conduct marketing activities, you will be duly informed and where we are legally required to obtain your consent to provide certain marketing materials, we will only provide with such marketing materials where we have obtained consent.

You will also receive the necessary information to opt out of us using personal information for marketing purposes by following the unsubscribe link included in each marketing email or by contacting us via email.

Disclosing your Personal Data to others

Sharing your Personal Data safely

We do not commonly share data with third-party. Shall we be in the situation where data sharing is necessary, you will be duly informed, and we will be not sharing data without a legal basis and namely your consent.

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

We do not allow our third-party service providers to use your Personal Data for their own purposes. We only permit them to process your Personal Data for specified purposes and in accordance with our instructions.

We ensure that the personal data being supplied is also limited with the minimum being used for each of the services provided by the third-party service providers.

Who we share Personal Data with

We may share your personal information with the following organisations that help us manage our business and deliver our products, applications, or services, or where we are legally obliged to share information, including with:

Twilio

- https://www.twilio.com/
  IVR voice to API calls - Sending only the limited input requests. Twilio storing the phone number only.
  More information can be found here https://www.twilio.com/gdpr
  It is used for SMS service/ insert link to pertinent page

Mailjet

Email SMTP server/ add link and pertinent information.

CRISP

is a third-party service provider to assist with Multichannel messaging platform (add available information/ Privacy notice/ website page with details on the used service)

Google

Google Storage and back end,

is a third-party service provider to assist us with client to store and back end the data necessary to provide MyC services/ insert link to google page with information on that type of processing.

DataDog

is a third-party service provider to assist us with client insight analytics
Used to tracking page views. Sending the 3rd party Page Information (URL, Title), Browser Information (Browser name, Viewport or Viewing pane, Screen resolution, Java enabled, Flash version), User Information (Location - IP address, Language).
More information can be found here https://www.datadoghq.com/legal/privacy/

GRCI Law

We use GRCI Law for data privacy services.

Law and Investigations

- Other organisations for the purposes of fraud/crime protection and investigation.
- Courts of law and government, regulatory authorities or third parties to the extent required by law, court order or a decision rendered by a competent public authority and for the purpose of law enforcement; or

Other

Other third parties subject to your consent.

Sharing your Personal Data overseas

We may send personal information outside of the Country/European Union generally for, but not limited to, reasons relating to processing and storage by our service providers. For example, we may have Cloud storage providers with data storage facilities in the US or other countries.

When we do this, we will ensure that our service provider has an appropriate level of protection, and the transfer is made in line with Data Protection Law. Often, this protection is set out under a contract with the organisation that receives that information. You can find more details of the protection given to your information when it is transferred overseas by contacting us.

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 that 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 periodically test the security of our systems to check for vulnerabilities.

Risk

Unfortunately, the transmission of information via the Internet is not completely secure. Although we will do our best to protect your Personal Data, we do not have any control over what happens between your device and the boundary of our information infrastructure. You should be aware of the many Information Security Risks that exist and take appropriate steps to safeguard your own information.

Encryption

All information you provide to us is stored encrypted in rest and in transit.

Breaches

We have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Third-party websites, plugins and services links to other websites

You should be aware that information about your use of this website (including your IP address) may be retained by your ISP (Internet Service Provider), the hosting provider and any third party that has access to your Internet traffic.

Our Website and Apps may contain links to third-party websites and plugins, for instance a social media login plugin. If you choose to use these websites, plugins, or services, you may disclose your information to those third parties.

We are not responsible for the content or practices of those websites, plugins, or services. The collection use and disclosure of your Personal Data will be subject to the privacy notices of these third parties and not this Privacy Notice. We urge you to read the privacy and cookie notices of the relevant third parties.

Use by children

We do not target children, and our Website, Services and Apps are not intended to attract children. Accordingly, our online services that collect Personal Data are not directed at and should not be accessed by individuals under the age of 18 years, and we request that such individuals do not provide any Personal Data to us, including via Cookies, please see our Cookie notice for further information.

Minors must obtain express consent from parents or legal guardians before accessing or providing any Personal Data. If notified by a parent or guardian, or discovered by other means, that a minor under the age of 18 has provided their Personal Data to us, we will delete the minor's Data that is in our possession.

Retention of your Personal Data

We will keep your Personal Data in line with our data retention policy for no longer than is 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 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.

You can contact us if you have questions relating to how long we will keep your personal data.

For more information on retention please refers to the CNIL related guidance.

Cookies

We use Cookies and similar technologies like pixels, tags, and other identifiers to remember your preferences, to understand how our Website and our Apps are used.

Further details can be found in our Cookie Notice.

Rights of data subjects

You have several rights under Data Protection Law. The rights available to you depend on our reason for processing your information and are set out in the Table of your rights.

Table of your rights

YOUR RIGHT	*DETAILS*
Right to be informed	We have a legal obligation to provide you with concise, transparent, intelligible, and easily accessible information about your personal information and our use of it. We have written this notice to do just that, but if you have any questions or require more specific information, you can contact us.
Right of access	You have the right to ask us for copies of your personal information. This right always applies. There are some exemptions, which means you may not always receive all the information. When you request this data, this is known as making a data subject access request (DSAR). In most cases, this will be free of charge; however, in some limited circumstances, for example repeated requests for further copies, we may apply an administration fee. Please contact us for more information or complete this **form** to exercise this right.
Right to rectification	You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies. Please contact us for more information or complete this **form** to exercise this right.
Right to erasure	You have the right to ask us to erase your personal information in certain circumstances. We have the right to refuse to comply with a request for erasure if we are processing the Personal Data for one of the following reasons: ● To exercise the right of freedom of expression and information. ● To comply with a legal obligation. ● To perform a task in the public interest or exercise official authority.

	● For archiving purposes in the public interest, scientific research, historical research or statistical purposes. ● For the exercise or defence of legal claims. Please contact us for more information or complete this **form** to exercise this right.
Right to restriction of processing	You may ask us to stop processing your Personal Data. We will still hold the data but will not process it any further. This right is an alternative to the right to erasure. If one of the following conditions applies, you may exercise the right to restrict processing: ● The accuracy of the Personal Data is contested. ● Processing of the Personal Data is unlawful. ● We no longer need the Personal Data for processing, but the Personal Data is required for part of a legal process. ● The right to object has been exercised and processing is restricted pending a decision on the status of the processing. Please contact us for more information or complete this **form** to exercise this right.
Right to object to processing	You have the right to object to processing in certain circumstances. You can also object if the processing is for a task carried out in the public interest, the exercise of official authority vested in you, or your legitimate interests (or those of a third party). Please contact us for more information or complete this **form** to exercise this right.
Right to data portability	This right only applies if we are processing information based on your consent or for the performance of a contract and the processing is automated. Please contact us for more information or complete this **form** to exercise this right.

How to exercise your rights

In most circumstances, you do not need to pay any charge for exercising your rights. We have one month to respond to you.

To exercise your rights or get more information about exercising them, please contact us, giving us enough information to identify you.

How you can complain to or about us

We hope that we can resolve any query or concern you raise about our use of your information. Please contact us first and title your email "***Complaint***". All complaints will be treated in a confidential manner and we will try our best to deal with your concerns.

You have the right to lodge a complaint with a supervisory authority in the EEA member states where you work or normally live, or where any alleged infringement of Data Protection Law occurred.

The supervisory authority in France is the CNIL which may be contacted following the instruction available here.
Details of supervisory authority based in other European Countries can be found here.

The Supervisory Authority in the UK is the ICO, which may be contacted at https://ico.org.uk/concerns or by telephone on 0303 123 1113.

Glossary

App(s)	App means an application that is a computer program or piece of software designed for a particular purpose that you can download onto a mobile phone or other device. Our Apps include - Webapps. A webapp is a web application (or web app). It is an application software that runs on a web server. - iOS App (Apple App Store) and Android App (Google Play Store).
CNIL	Commission Nationale de l'Informatique et des Libertés (CNIL)
Consent	The UK GDPR and EU GDPR. sets a high standard for consent , consent should be given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. ● What are the GDPR consent requirements? - GDPR.eu ● Art. 7 GDPR - Conditions for consent - GDPR.eu ● Recital 43 - Freely given consent - GDPR.eu
Controller	means the natural or legal person, public authority, agency or any other entity or person who alone or jointly with others determines the purposes and means of the processing of personal data.
Cookies	means a small file of letters and numbers that is stored on a browser or the hard drive of a computer. Cookies contain information that is transferred to a computer's hard drive. Controllers must have users' informed consent before storing cookies on a user's device and/or tracking them. For more information, please read our cookie notice.

	Additional information on Cookies can be found on the CNIL related webpages.
DPA	Data Protection Authority such as CNIL and ICO also known as Supervisory Authority
Data Protection Law	means all applicable data protection and privacy legislation in force from time to time including the UK GDPR and the EU GDPR, the Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the national implementing legislation and any other legislation relating to personal data and all other legislation and regulatory requirements in force from time to time that apply to the use of personal data.
Encryption	is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information. For more information see the CNIL related webpages.
e-Privacy Directive/Regulation	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). A proposal for a e-privacy Regulation is currently under discussion
EU GDPR	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing the Directive. General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)
ICO	means the Information Commissioner's Office, the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Home | ICO
Information Security Risks	comprises the impacts on individuals or organisations that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate. ● Top 10 risks to include in an information security risk assessment (vigilantsoftware.co.uk) ● Art. 32 GDPR - Security of processing - GDPR.eu
Joint Controller	A joint Controller relationship arises where two or more Controllers jointly determine the purposes and means of the processing of personal data
Lawful Basis	under the EU GDPR and the UK GDPR, you must have a valid lawful basis to process personal data.

	Lawful Basis of processing personal data Level 2 Heading] There are six lawful bases for processing personal data available: (a) **Consent**: the individual has given clear consent to the processing of their personal data for a specific purpose. (b) **Contract:** the processing is necessary for a contract, or because specific steps have been taken before entering into a contract. (c) **Legal obligation:** the processing is necessary for compliance with the law (not including contractual obligations). (d) **Vital interests**: the processing is necessary to protect someone's life. (e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (f) **Legitimate interests:** the processing is necessary for an organisation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. (This cannot apply if an organisation is a public authority processing data to perform its official tasks.) **For more information** Art. 6 GDPR – Lawfulness of processing GDPR: lawful bases for processing, with examples - IT Governance UK Blog **Special category data** Special category data is personal data that needs more protection because it is sensitive. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 of the UK GDPR and EU GDPR and a separate condition for processing under Article 9. These do not have to be linked.
Legitimate Interests Assessment (LIA)	is a form of risk assessment and should be conducted by an organisation when your personal data processing is based on legitimate interest. The LIA is split into three steps: ● Assessing whether a legitimate interest exists. ● Establishing the necessity for processing. ● Performing the balancing test. For more information on Legitimate interest you can refer to the CNIL related webpage.
Personal Data	this is also referred to as "*personal information*" and it means any information relating to an identified or identifiable natural person ('**data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the

	physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. ● Art. 33 GDPR - Notification of a personal data breach to the supervisory authority - GDPR.eu
Privacy Notice	(also sometimes called a privacy policy or fair processing notice) is a public document from an organisation that explains how that organisation processes personal data and how it applies data protection principles under Articles 12, 13 and 14 of the EU GDPR and the UK GDPR.
Processor	Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. Processors act on behalf of the relevant Controller and under their authority.
Special Category Personal Data	some of the personal data that organisations process is more sensitive and needs higher protection. Under the GDPR, this is known as '***special categories of personal data***', and includes information about a person's: ● Race ● Ethnicity ● Political views ● Religion, spiritual or philosophical beliefs ● Biometric data for ID purposes ● Health data ● Sex life data ● Sexual orientation ● Genetic data In order to lawfully process special category personal data, we must identify both a lawful basis under Article 6 of the UK GDPR and EU GDPR and a separate condition for processing under Article 9. These do not have to be linked. There are ten conditions for processing special category data in Article 9 of the EU GDPR and the UK GDPR .
Special Category Personal Data Conditions for Processing	the conditions for processing special category data: (a) Explicit consent (b) Employment, social security and social protection (if authorised by law) (c) Vital interests (d) Not-for-profit bodies (e) Made public by the data subject (f) Legal claims or judicial acts (g) Reasons of substantial public interest (with a basis in law) (h) Health or social care (with a basis in law)

	(i) Public health (with a basis in law) (j) Archiving, research and statistics (with a basis in law) ● Art. 9 GDPR - Processing of special categories of personal data - GDPR.eu ● GDPR | Personal Data vs Sensitive Data: What's the Difference? (itgovernance.co.uk)
Supervisory Authorities	means the data protection authority tasked with supervising GDPR compliance in each member state of the European Union. What are Data Protection Authorities (DPAs)? | European Commission (europa.eu)
Tracking Pixels	a tracking pixel is an HTML code snippet which is loaded when a user visits a website or opens an email. It is useful for gathering information about visitors on a website—how they browse, what type of ads they click on, etc.
UK GDPR	means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018, together with the DPA 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and other data protection or privacy legislation in force from time to time in the United Kingdom. The UK GDPR | ICO
Website	https://www.myc.doctor/ https://app-eu.myc.doctor https://app.myc.doctor