Life-GP
167-169 Great Portland Street
London
W1W 5PF

Email: info@life-gp.com

UK GDPR Policy

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Life-GP.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Life-GP.

B. Document Details

Document Reference:	Life-GP GDPR / Privacy Policy
Current Version Number:	v1.2
Current Document Approved By:	Dr Corinne Fletcher
Date Approved:	Jan 2024

UK GDPR Policy

Table of contents

1 Introduction

1.1 POLICY STATEMENT

The UK General Data Protection Regulation (UK GDPR herein) came into force on 1 January 2021 and is incorporated in the Data Protection Act 2018 (DPA18) at part 2. The UK GDPR applies to all organisations in the UK (with the exception of law enforcement and intelligence agencies) and Life-GP must be able to demonstrate compliance at all times. Understanding the requirements of the UK GDPR will ensure that the personal data of both staff and clients is protected accordingly.

1.2 Status

Life-GP aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.3 Training and support

Life-GP will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

This document applies to all who work at Life-GP and other individuals performing functions in relation to LifeGP.

2.2 Why and how it applies to them

All personnel at Life-GP have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the UK GDPR.

3 Definition of terms

3.1 Consent

Consent of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[1]

3.2 Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation (UK GDPR).[2]

3.3 Data protection by design and default

Data protection by design and default means putting in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.[3]

[1] Article 4 UK GDPR
[2] ICO About the DPA 2018
[3] ICO Guide to the UK General Data Protection Regulation

3.4 Data Protection Officer

An expert on data privacy, working independently, to ensure compliance with policies and procedure.

3.5 Data controller
The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.[4]

3.6 Data processor
A natural, or legal person, public authority, agency or other body that processes personal data on behalf of the controller.[4]

3.7 Data subject
The identified or identifiable living individual to who personal data relates.[5]

3.8 UK General Data Protection Regulation (UK GDPR)
The UK GDPR sets out the key principles, rights, and obligations for most processing of personal data in the UK.[3]

3.9 Personal data
Information that relates to an identified or identifiable individual.[6]

3.10 Personal data breach
A 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.[2]

3.11 Processing
Any operation or set of operations that is performed on personal data or on sets of personal data whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.12 Pseudonymisation
Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.[6]

3.13 Recipient
The entity to which personal data is disclosed.

4 Introduction of the UK GDPR

4.1 Background
The UK GDPR was introduced on 1 January 2021 and is largely based on the EU GDPR which had applied in the UK since 25 May 2018.

4.2 UK GDPR and DPA18
The UK GDPR is incorporated in the DPA18 at Part 2.

[4] Article 4 UK GDPR
[5] ICO Definitions
[6] ICO What is personal data

5 Data protection by design and default

5.1 Data protection by design

Data protection by design is a legal requirement and is an approach that ensures that privacy and data protection issues are considered at the design phase of any system, service, product, or process and then throughout the lifecycle.[3]

Life-GP will demonstrate data protection by design by:

- Conducting a data protection impact assessment (DPIA).
- Ensuring there are privacy notices on the website and in the waiting rooms which are written in simple, easy-to-understand language.
- Adhering to Articles 25(1) and 25(2) of the UK GDPR[7].
- Adhering to Section 6.1 of this policy.

Data protection by design is a legal requirement.

5.2 Data protection by default

Data protection by default is an approach that ensures that data is processed only for the achievement of a specific purpose.[3]

Life-GP will demonstrate data protection by default by:

- processing data only for the purpose(s) intended,
- ensuring consent is obtained from the data subject prior to data being processed,
- providing clients access to their data on request (Subject Access Requests),
- ensuring clients consent to access of their data by third parties,
- processing data in a manner that prevents data subjects being identified unless additional information is provided (using a reference number as opposed to names – pseudonymisation), and
- processing data in accordance with section 6.2 of this policy.

Through effective data protection Life-GP will remain compliant with the UK GDPR.

6 Roles of data controllers and processors

6.1 Data controller

At Life-GP, the role of the data controller is to ensure that data is processed in accordance with Article 5 of the UK GDPR. They should be able to demonstrate compliance and is responsible for making sure that data is:[8]

- processed lawfully, fairly and in a transparent manner in relation to the data subject,
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,
- adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed,

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay,
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed, and

[7] Article 25 UK GDPR

[8] Article 5 Principles relating to processing of personal data

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The data controller at Life-GP is the registered manager.

6.2 Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:[9]

- the data subject has given consent to the processing of his/her personal data for one or more specific purposes,
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- processing is necessary for compliance with a legal obligation to which the data controller is subject
- processing is necessary in order to protect the vital interests of the data subject or another natural person,
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
- processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

At Life-GP, all staff are classed as data processors as their individual roles will require them to access and process personal data.

7 Data subjects' rights

7.1 Overview

All data subjects have the following rights[10]

1. the right to be informed,
2. the right of access,
3. the right to rectification,
4. the right to erasure,
5. the right to restrict processing,
6. the right to data portability,

7. the right to object, and
8. rights in relation to automated decision making and profiling.

7.2 Right to be informed

In accordance with Articles 13 and 14 of the UK GDPR, Life-GP is obliged to advise data subjects of the purposes for processing their data, the retention periods for the data and who this data will be shared with. This is referred to as privacy information.

7.3 Right of access

Life-GP ensures that all clients are aware of their right to access their data and will have privacy notices displayed on the Life-GP website.

[9] Article 6 Lawfulness of processing [10]
ICO - Individual Rights

To comply with the UK GDPR, all organisation privacy notices are written in a language that is understandable to all clients and meet the criteria detailed in Articles 12, 13 and 14 of the UK GDPR.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

7.4 Right to rectification

In accordance with Article 16 of the UK GDPR, data subjects have the right to have inaccurate personal data rectified and/or incomplete personal data completed.

A request can be verbal or in writing and the Information Commissioner's Office (ICO) recommends that any request is followed up in writing as this will allow the requestor to explain their concerns, give evidence and state the desired solution. Additionally, this will also provide clear proof of the requestor's actions, should they decide to challenge Life-GP's initial response.

Detailed guidance from the ICO can be accessed here.

7.5 Right to erasure

In accordance with Article 17 of the UK GDPR, data subjects have the right to have personal data erased (this is also referred to as the right to be forgotten). This right permits a data subject to request personal data is deleted in situations where there is no compelling reason to retain the data.

Where Life-GP has shared information with a third party, there is an obligation to inform the third party about the data subject's request to erase their data providing it is achievable and reasonably practical to do so. Detailed guidance can be accessed here.

7.6 Right to restrict processing

In accordance with Article 18 of the UK GDPR, individuals have the right to restrict the processing of their personal data. This applies in certain circumstances, with the aim being to enable the individual to limit the way an organisation processes (uses) their data. This right can be used as an alternative to the right to erasure.

7.7 Right to data portability

The right to data portability permits data subjects to receive and reuse their personal data for their own purposes and across different services.

7.8 Right to object

In accordance with Article 21 of the UK GDPR, individuals have the right to object to the processing of their personal data at any time. At Life-GP, individuals are requested to provide specific reasons why they object to the processing of their data. If the reasons are not an absolute right, Life-GP can refuse to comply. See the ICO guidance for detailed information.

7.9 Rights in relation to automated decision making and profiling

In accordance with Article 22 of the UK GDPR, Life-GP, is not permitted to make solely automated decision making. This includes profiling.

[1] Subject access requests

"An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data."

Any requests not using the SAR form, must be processed.

8.2 Responding to a subject access request

In accordance with the UK GDPR, data controllers must respond to all data subject access requests within one month of receiving the request. It is the guidance of the ICO that a universal approach is applied and a 28-day response time implemented.[2] At Life-GP, the 28-day response time applies.

In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.

Should the request involve a large amount of information, the data controller will ask the data subject to specify what data they require before responding to the request. Data controllers are permitted to 'stop the clock' in relation to the response time until clarification is received.

8.3 Fees

Under the UK GDPR, Life-GP is not permitted to charge data subjects for initial access; this must be done free of charge. In instances where requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive" a reasonable fee may be charged. However, this does not permit Life-GP to charge for all subsequent access requests.[3]

The fee is to be based on the administrative costs associated with providing the requested information.

---

[1] **.1 Recognising subject access requests**

At Life-GP, data subjects are encouraged to use the subject access request (SAR) form which is included in the access to medical records policy. All staff must note that the ICO state:

[2] ICO Right of access

[3] BMA Guidance – Access to health records

8.4 Verifying the subject access request

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures.

The use of Life-GP's Subject Access Request (SAR) form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e., driving licence, or passport.

8.5 Supplying the requested information

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

Should an individual submit a SAR electronically, Life-GP will reply in the same format (unless the data subject states otherwise).

8.6 Third party requests

At Life-GP, the data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject.

The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject.

8.7 Requests from solicitors

At Life-GP, requests are received from third parties such as solicitors. It is the responsibility of the third party to provide evidence that they are permitted to make a SAR on behalf of their client. If concern or doubt arises, Life-GP will contact the client to explain the extent of disclosure sought by the third party.

Life-GP can then provide the client with the data as opposed to directly disclosing it to the third party. The client is then given the opportunity to review their data and decide whether they are content to share the information with the third party.

8.8 Refusing to comply with a SAR

Life-GP will only refuse to comply with a SAR where exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- the reasons why the SAR was refused,
- their right to submit a complaint to the ICO, and
- their ability to seek enforcement of this right through the courts

Each request must be given careful consideration and should Life-GP refuse to comply, this must be recorded and the reasons for refusal justifiable.

9 Data breaches

9.1 Data breach definition

A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data.[13]

Examples of data breaches include:

- access by an unauthorised third party,
- deliberate or accidental action (or inaction) by a data controller or processor,
- sending personal data to an incorrect recipient,
- loss or theft of computer devices containing personal data, • alteration of personal data without permission, or
- loss of availability of personal data.

Examples of data breaches can be found on the ICO website.

9.2 Reporting a data breach

At Life-GP, should any member of staff become aware of a data breach they are, where possible, to contain the breach and advise the data controller immediately.

When determining whether Life-GP needs to report the data breach to the ICO, this decision is to be based on whether the breach is a high risk to an individual's rights and freedoms. If this is deemed to be the case, then the ICO will need to be notified.

Whatever decision is made, Life-GP must be able to justify the decision.

Breaches are to be reported to the ICO without undue delay or within 72 hours of becoming aware of the breach.

Failure to report a breach can result in a fine of up to £8.7m. It is therefore imperative that there are effective processes in place at Life-GP to detect, investigate and report breaches accordingly.

[13] ICO – Personal data breaches

The data controller is to ensure that all breaches at Life-GP are recorded. Article 33 of the UK GDPR outlines the requirements which include:

- recording the facts pertaining to the breach,
- the effects the breach has had on individuals or organisations,
- any remedial action(s) that have been completed,
- the cause of the breach i.e., system or human error, and
- considering what system or process changes may be required to prevent future incidences.

9.3 Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e., a breach that is likely to have an adverse effect on an individual's rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at Life-GP is to provide the data subject with the following information in a clear, comprehensible manner:

- the circumstances surrounding the breach,
- the details of the person who will be managing the breach,
- any actions taken to contain and manage the breach, and • any other pertinent information to support the data subject.

10 Consent

10.1 Appropriateness

The UK GDPR states that consent must be unambiguous and requires a positive action to "opt in" and it must be freely given. Data subjects have the right to withdraw consent at any time.

10.2 Obtaining consent

Consent is one of the lawful bases of processing and is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[14] If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- why Life-GP wants the data,
- how the data will be used by the organization,
- the names of any third party data controllers with whom the data will be shared, and • their right to withdraw consent at any time.

All requests for consent are to be recorded, with the record showing:

- the details of the data subject consenting,
- when they consented,
- how they consented, and
- what information the data subject was told.

Consent is to be clearly identifiable and separate from other comments entered into the care record. At LifeGP, it is the responsibility of the data controller to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (clients) are fully aware of their right to withdraw consent and must facilitate withdrawal as and when it is requested.

[14] ICO Consent

11 Summary

Given the complexity of the UK GDPR, all staff at Life-GP must ensure that they fully understand the requirements within the regulation. Understanding the regulation will ensure that personal data at Life-GP remains protected and the processes associated with this data are effective and correct.