Policies & Principles

The GDPR updates the data protection principles from the previous Data Protention Act 1998 (DPA) but largely addresses the same issues albeit with some expansion. Afya Care will adhere to these principles and they should be borne in mind when seeking to comply with the GDPR.

1. Personal information shall be processed lawfully, fairly and in a transparent manner
2. Personal information shall be collected for specified, explicit and legitimate purposes
3. Personal information shall be adequate, relevant, and limited to what is necessary
4. Personal information shall be accurate and where necessary, kept up-to-date
5. Personal information shall be retained only for as long as necessary
6. Personal information shall be processed in an appropriate manner to maintain security

The Afya Care has responsibility for making sure that all employees have read and understand the IG and IT Policies and will ensure that local impacts are considered and local procedures amended to comply. As an employee you will be asked to initial a tracking sheet to say that you have read and understood relevant policies.

Look out for further posters and emails on GDPR and should you require more information you can reach out to your Manager.

What is personal data?

The key terms

GDPR and other data protection laws rely on the term 'personal data' to discuss information about individuals. There are two key types of personal data in the UK and they cover different categories of information.

What is personal data?

Personal data can be anything that allows a living person to be directly or indirectly identified. This may be a name, an address, or even and IP address. It includes automated personal data and can also encompass pseudonymised data (this means replacing any identifiying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified) if a person can be identified from it.

So, what's sensitive personal data?

GDPR calls sensitive personal data as being in 'special categories' of information. These include but are not limited to trade uniion membership, religious beliefs, political opinions, racial information and sexual orientation.

What's the difference between a Data Controller and Data Processor?

The GDPR distinguishes and defines clear responsibilities for those organisations that own the data and those that may process it on behalf of another and these are defined as:

- **Data Controller** - A controller is an entity that decides the purpose and manner that personal data is used, or will be used.
- **Data Processor** - The person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data. Both Data Controllers and Processors have obligations to inform ICO of breaches and can both be subject to fines and sanctions.

What does GDPR mean for you?

GDPR does not just impact you in the work place but it also has implications for your own access to your own data held by any organisation.

As well as putting new obligations on the companies and organisations collecting personal data, the GDPR also gives individuals a lot more power to access the information that's held about them. At present a Subject Access Request (SAR) allows businesses and public bodies to charge £10 to be given what's held about them, but going foward this will be free.

When someone asks a business for their data, they must provide the information within one month.

The new regulation also gives individuals the power to get their personal data erased in some circumstances.

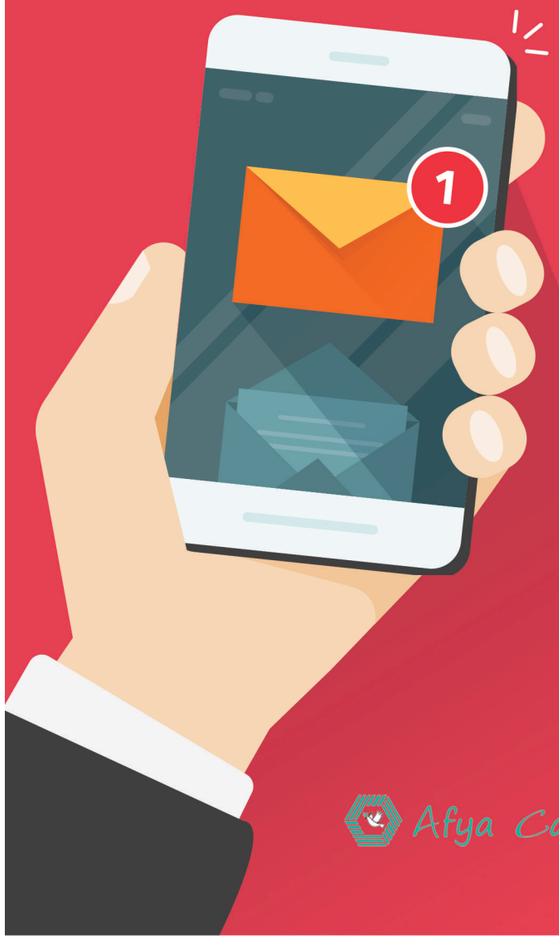
Ressons can be:

- Where it is no longer necessary for the purpose it was collected
- If consent is withdrawn
- There's no legitimate interest
- If it was unlawfully processed

Going forward organisations will need to obtain more explicit consent to contact/market to you and many will need to re-request your consent over email and letter.

Understanding GDPR

for Afya Care Employees



Afya Care

What is GDPR exactly?

The General Data Protention Regulation (GDPR) is a European Union initiative which brings Data Protention Law into the 21st Century harmonising data protection law across Europe and affecting any organisation anywhere in the world that wants to do business with Europe. The UK will bring this into UK Law in May 2018 replacing the existing Data Protention Act 1998, and Afya Care has aligned itself to the new legislation. The GDPR builds on the principles of the current UK Data Protention Act and extends the definition of personal data and enhances individual rights and protections.

The facts:

Who will enforce it in the UK?

The information Commissioner's Office (ICO) is the UK Goverment body to which organisations will answer to and they have the power to hand out significant fines and data processing sanctions.

Why do we need this change and what's new?

The use and volume of personal data has increased massively in last 20 years, as has the ability to exploit and misure that information. The new law will provide greater transparency, enhanced access and privacy rights for individuals and increased accuntability for organisations.

Does Brexit matter?

The UK will adopt the GDPR within a new Data Protention Bill and has committed to staying aligned to EU Data Protention Law.

How is Afya Care impacted?

The new legislation puts a greater emphasis and obligation to deliver this consistently and reliably across all areas of our Business and be able to evidence our compliance to an even greater extent.

Afya Care will meet its GDPR obligations from the start date, but this is a journey and over the coming months and years, data protection and IT Security will become more a part of our everyday work place.
Everyone in Afya Care has a duty to make themselves aware of the GDPR Principles and Afya Care & IT Security Policies.

"Everyone in Afya Care has a duty to make themselves aware of the GDPR Principles and Afya Care & IT Security Policies."

How have we prepared for GDPR?

- **Carrying out an information audit.** We have identified exactly what information we collect, where it's stored, how it's protected, who we share it with and what it's used for.
- **Getting the right policies in place.** we have created clear information and it securiteies policies for the collection, storage, sharing and management of information.
- **Document what we collect and why.** We have defined business information flows and creaded an Information Asset Register to document what we collect, for that purpose, the legal basis for collection, what we do with it and how long we hold onto it for.
- **Understanding how we process data.** We have documented what we do with the information we hold and where and how it is stored.
- **Protecting the data we hold.** We have undertaken a security review of our IT systems to ensure electronic information is secure and improved local processes for handling and managing physical information assets.
- **Updating our employee & supplier contracts.** We are ensuring that our employee and third-party contracts contain provisions to protect the information or our employees and those we care for.
- **Privacy policy.** We have updated Privacy policies to describe to our job applicants, employees, client and relatives what information Afya Care collects and why, how it is used, what their rights are and how they can access saved information.
- **Understanding our Clients and employees' rights.** We have produced guidance for employees, clients and their families individual rights.
- **Ensuring we get appropriate consent.** We are rolling out a robust consent process for marketing and communication materials, so that we get permission from our clients to collect their information when required.

How do we manage Afya Care data?

- **Know what data you have, and why you have it** - only capturing data we need.
- **Manage data in a structured way** - following Afya Care policies and procedures.
- **Know who is responsible for it** - assign Information Asset Owners for all data so that it is clearly managed and governed.
- **Be Security and Information Governance aware** - ensure that ourselves and our team have had the necessary training.

What trainging is abailable?

Information Governance Awareness Training - All afya Care employees will be offerd training and this will bring out IG and IT security policies, whihc have been aligned to GDPR. the training will cover how we handle and share information, how we keep our Desk and IT equipment secure and how we manage, archive and dispose of the information we hold.

How does GDPR impact on how we communicate?

Opt in, not out - explicit consent required - to gain data consent from Clients, families and potential Clients use their data we will have to use clear opt-in tick boxes, that state clearly what and how we will communicate with them.