

Force24 GDPR Compliance and Guidance Statement

Date of Issue
January 26 2018
V1.4

Force24™
Marketing Automation

Index

04 Force24 And Our Internal Compliance

06 Documents, Policies And Procedures

08 Force24'S Gdpr Compliance Journey

10 Transferring Data

12 The Right To Be Informed

14 The Right Of Access

16 The Right To Rectification

18 The Right To Erasure (Or Be Forgotten)

20 The Right To Restrict Processing

22 The Right To Data Portability

24 The Right To Object

26 Rights In Relation To Automatic Decision Making & Profiling

28 Definitions, Legal Notes And Gdpr Support

Introduction

The General Data Protection Regulation (GDPR) is looming and Force24 is working tirelessly to ensure the service provided for clients is totally compliant through the introduction of additional new policies, processes and technical controls. Whilst the new regulations are demanding, rigorous and perhaps for some a little daunting, the key to meeting GDPR compliance at Force24 is through investing in personnel, systems, staff training, technical controls and new documented procedures.

At the heart of GDPR is personal data protection by design and default. This is different to earlier legislation, and has required a total rethink by Force24 to ensure that the protection of personal data is at the centre of everything it does.

Force24 believes that its UK hosted marketing technology and automation platform is fundamental to ensuring your marketing activities are always GDPR compliant.

This privacy guidance statement is designed to answer the specific elements affecting marketers working with Marketing Automation. Below is an overview of the key themes you need to consider, and Force24's solution to each of these requirements.

Force24 And Our Internal Compliance

Force24 embarked on the journey of becoming GDPR compliant during 2017. Force24 sees GDPR as a potential milestone in marketing history: the date marketing was changed for the better.

Force24 believes the first step in ensuring our clients are compliant is to ensure that its own business is an unrivalled example of compliance.

Our journey began with the appointment of a certified GDPR practitioner (Philip Allott). Philip has also been appointed as the Force24 DPO (Data Protection Officer), holding overall responsibility for the practices and policies upheld and operated by Force24.

During the GDPR journey, all departments of the Force24 team have been involved in defining our policies, processes and technical controls.

All Force24 clients have access to download these documents through the help section of the portal.



Documents, Policies And Procedures

As part of the verification process, Force24 would like to make available to you all its internal documents, policies and procedures relating to data categorisation, data protection and data processing.

Anti-Bribery Policy - V1.2

Force24's Anti-Bribery Policy concerns the acceptance of gifts and bribes for attempted access to personal information. It is designed to maintain the highest possible standards of business practice, and to highlight the Company's 'zero-tolerance' to bribery.

Business Continuity Plan - V1.1

This extensive 24-page document sets out in detail Force24's strategy and plans to ensure business continuity and the protection of data in the event of a crisis.

Data Classification Handbook - V1.5

The Data Classifications Handbook is designed to ensure members of staff understand how to handle client information. Six categories of data are covered ranging from Ultra – Secret to public documents, along with appropriate security safeguards and restricted access rights for each listing.

Data Compliance Handbook - V1.1

This handbook details the hardware and software protocols for protecting client data. It covers everything from firewalls and password protection to backups and is designed to be used in association with the data classification handbook.

Data Protection Policy - Internal Procedures - V1.4

The document outlines Force24's policies and procedures concerning data protection and access rights, following the introduction of GDPR. This document relates specifically to both employer and employee responsibilities concerning GDPR. Force24 believes that the lawful and correct treatment of personal information is vitally important to the achievement of the company's objectives, the success of the business, and to maintaining the confidence of those with whom it trades. Force24 requires all personal information to be handled lawfully and correctly.

Data Storage Retention and Disposal Policy - V1.4

Force24's Data Storage, Retention and Disposal Policy outlines in detail the approach the business takes to the storage of client data along with the disposal policy, post data usage.

Equipment Standards Policy - V1.3

This brief document outlines minimum hardware standards, including which browsers are supported.

Information Security Policy - V1.7

At Force24, security is everyone's responsibility and this highly detailed document provides clear direction concerning the protection of client data and GDPR responsibilities. Security is treated as part of the employee's daily routine and employees are mandated to take appropriate security measures to protect any personal data and its storage at all times.

Internet Usage Policy – V1.1

The Internet Usage Policy applies to all employees of Force24 who have access to computers and the Internet, used in performance of their work. Strict rules apply concerning the sending of data which is GDPR compliant. All employees are required to sign the document, and disciplinary action and dismissal could result if there is a data breach.

Staff Security and Awareness Handbook - V1.5

A plain English approach for all staff members, which they are required to sign, to ensure they are keep abreast of their data protection responsibilities under GDPR and Force24's security protocols.

Trust and Confidentiality Agreement - V1.1

This legally enforceable document places strict obligations on all Force24 employees concerning the handling of client information and especially personal data. GDPR compliance is a binding obligation.

Wireless LAN Security Policy – V1

The policy covers all wireless data communication devices physically connected to any of Force24's internal networks. This includes any form of wireless communication device capable of transmitting packet data. It is a Force24 disciplinary offence to violate the policy.

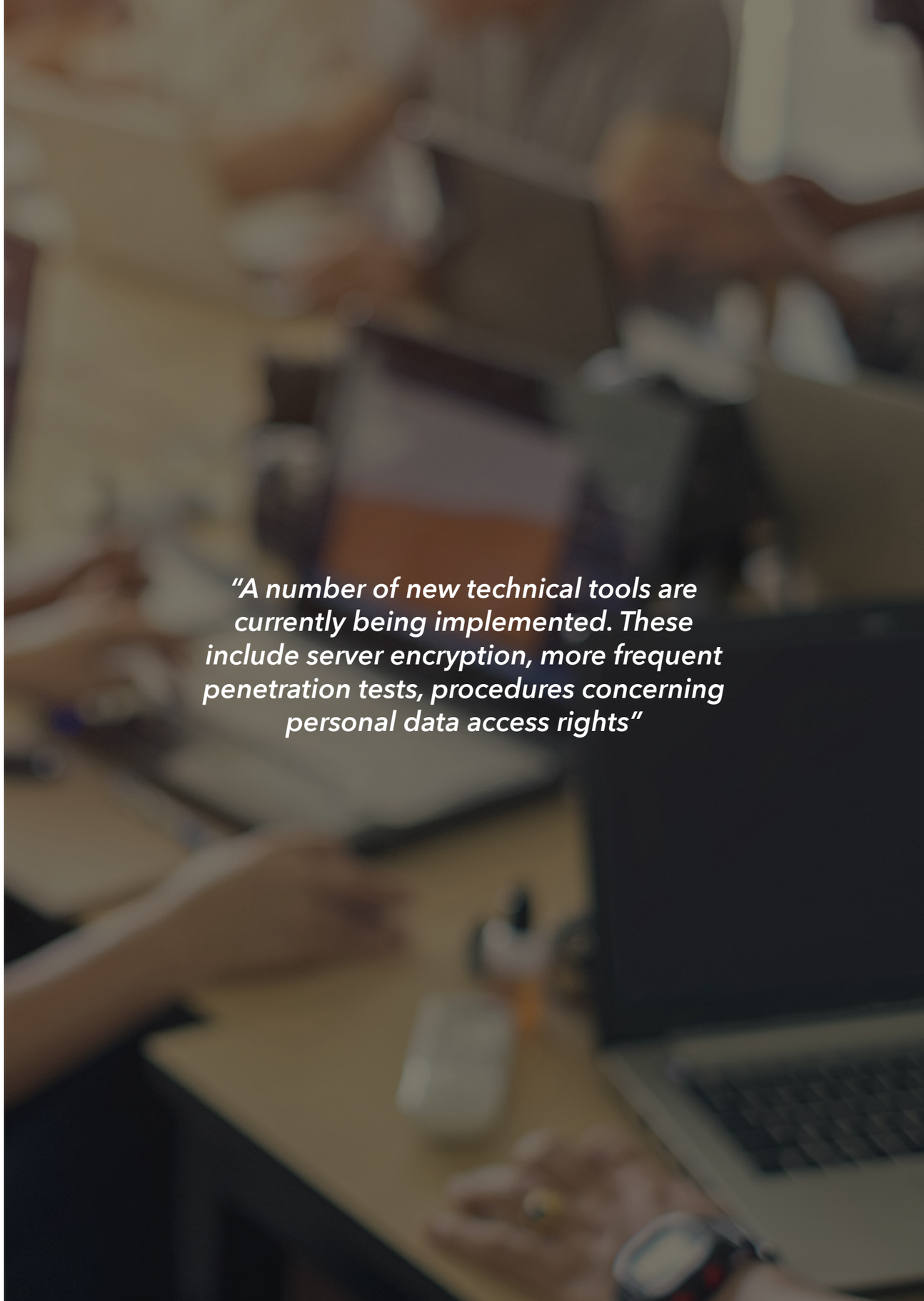
Force24'S GDPR Compliance Journey

Although Force24's compliance journey currently continues. This will shortly be completed. The work undertaken started with a complete audit by a qualified GDPR Practitioner, to identify any anomalies and to recommend best practice concerning policies, processes and the technical controls required to meet the enhanced data protection standards required by GDPR.

During the course of the last few months, Force24 has implemented new policies, including amendments to staff contracts, contractual arrangements, data protection and the updating of numerous documents to make them GDPR compliant.

A number of new technical tools are currently being implemented. These include server encryption, more frequent penetration tests, procedures concerning personal data access rights, the creation of strict data management procedures and the introduction of secure file transfer protocol (SFTP) for future data transfers.

New processes currently in progress include the auditing of suppliers, staff training and working closely with clients who are controlling personal data, to ensure they have the necessary permissions in place to run b2c campaigns.



Transferring Data

What does this mean?

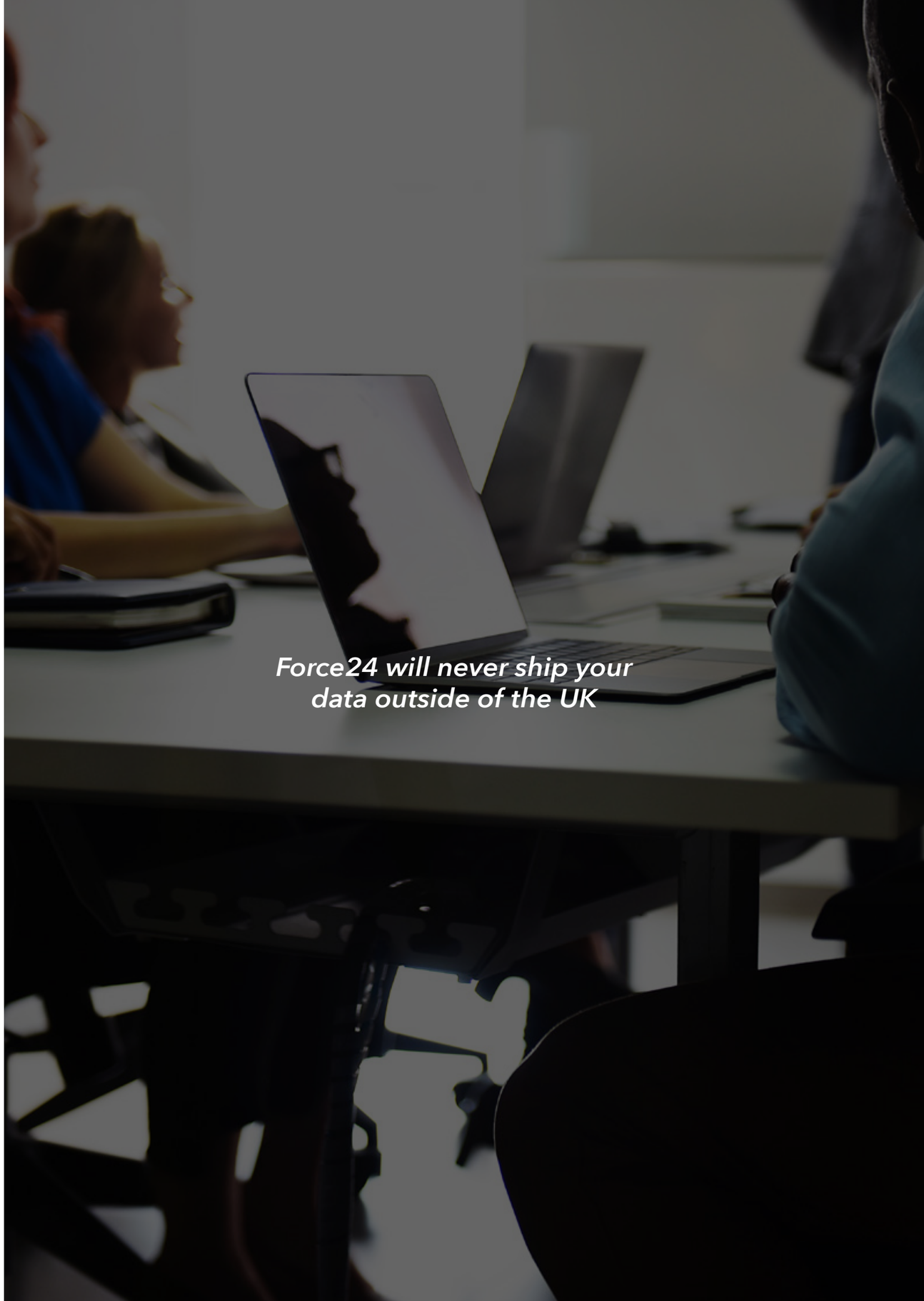
GDPR imposes very strict restrictions on the transfer of personal data outside of the EU. This is to ensure citizens can be assured that the level of protection GDPR provides cannot be undermined by external countries or international organisations.

Under GDPR data can only be moved outside the EU to countries within the EEA and the following additional countries which are considered by the EU as having adequate data protection laws: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Authorisation to send personal data to other countries is only possible with the permission of the Information Commissioner's Office and/or the European Commission, or for intercompany transfers using Binding Corporate Rules (BCR). Data transfers should not be made to the United States unless the recipient has signed the US Privacy Shield. Certain derogations are possible where companies have obtained the explicit consent of the data subject, or it is part of a legal defence or for certain other limited permissible reasons. Failure to have the right documentation in place and permission could result in a fine of up to €20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is higher).

It is important to note that the use of US Marketing Automation platforms and others cloud based solutions based in the US or elsewhere in the world could result in you exposing your organisation to a serious fine.

How does Force24 help?

Force24 will never ship your data outside of the UK. Force24's infrastructure is held within London and Glasgow. All support professionals are located within the UK and EU member countries.



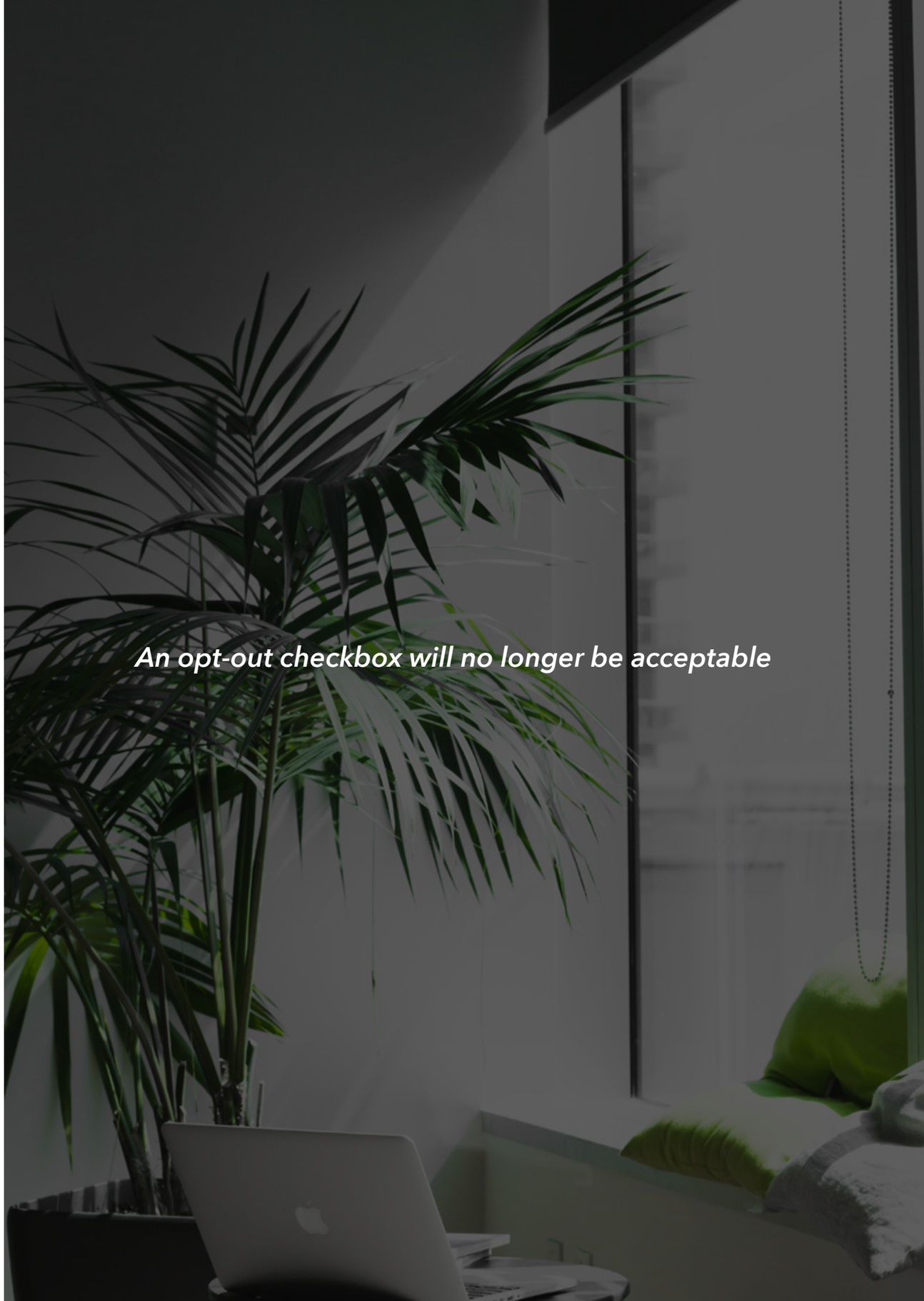
The Right To Be Informed

What does this mean?

This refers to your obligation to provide ‘fair processing information’, typically through a privacy notice. The information provided about the processing of personal data must be concise, transparent, intelligible and easily accessible, written in clear and plain language. Your customers and prospects will need to give you “unambiguous” permission, and a pre-ticked opt-in checkbox will no longer be permissible. Customers will need to deliberately opt-in to receive communications from you and be clear on what messaging they will receive. You will need to be able to prove this by keeping audit trails for all personal data that outlines when permission was granted and for what.

How does Force24 help?

Force24’s GDPR practitioner is developing a data processing document and a simple set of data collection guides, showing the most optimised yet fully compliant procedures. Once established, all clients will automatically inherit this process for all of the data capturing points managed within the Force24 platform. All Force24 customers will have access to these documents on their release which will govern all external data collection points.



The Right Of Access

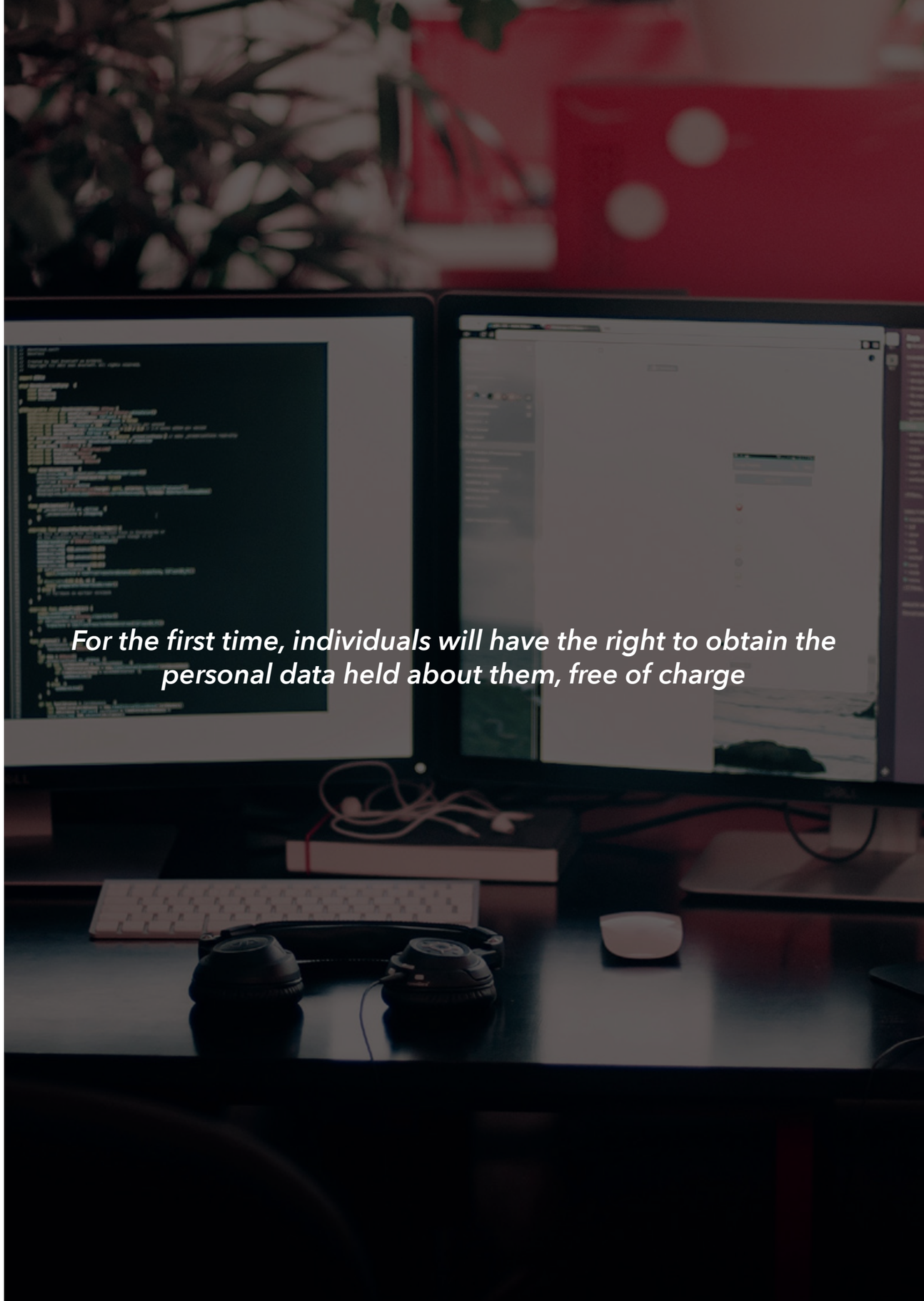
What does this mean?

Data subjects (individuals) will have the right, often for the first time, to obtain the personal data held about them free of charge. You will need to ensure that you have a holistic view of where the personal data you hold on someone is being used, stored and exactly where in your business, as people will have the right to request confirmation that you're processing their data, for what reason and where. Information must be provided within one month of the request.

How does Force24 help?

Force24 has implemented a free to access report detailing all information held on any individual contact. The report may be requested at any time and will be delivered within two working days of your request. The report will be transmitted via a protected XLSX file for your onward transit to the necessary recipient.

PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access



The Right To Rectification

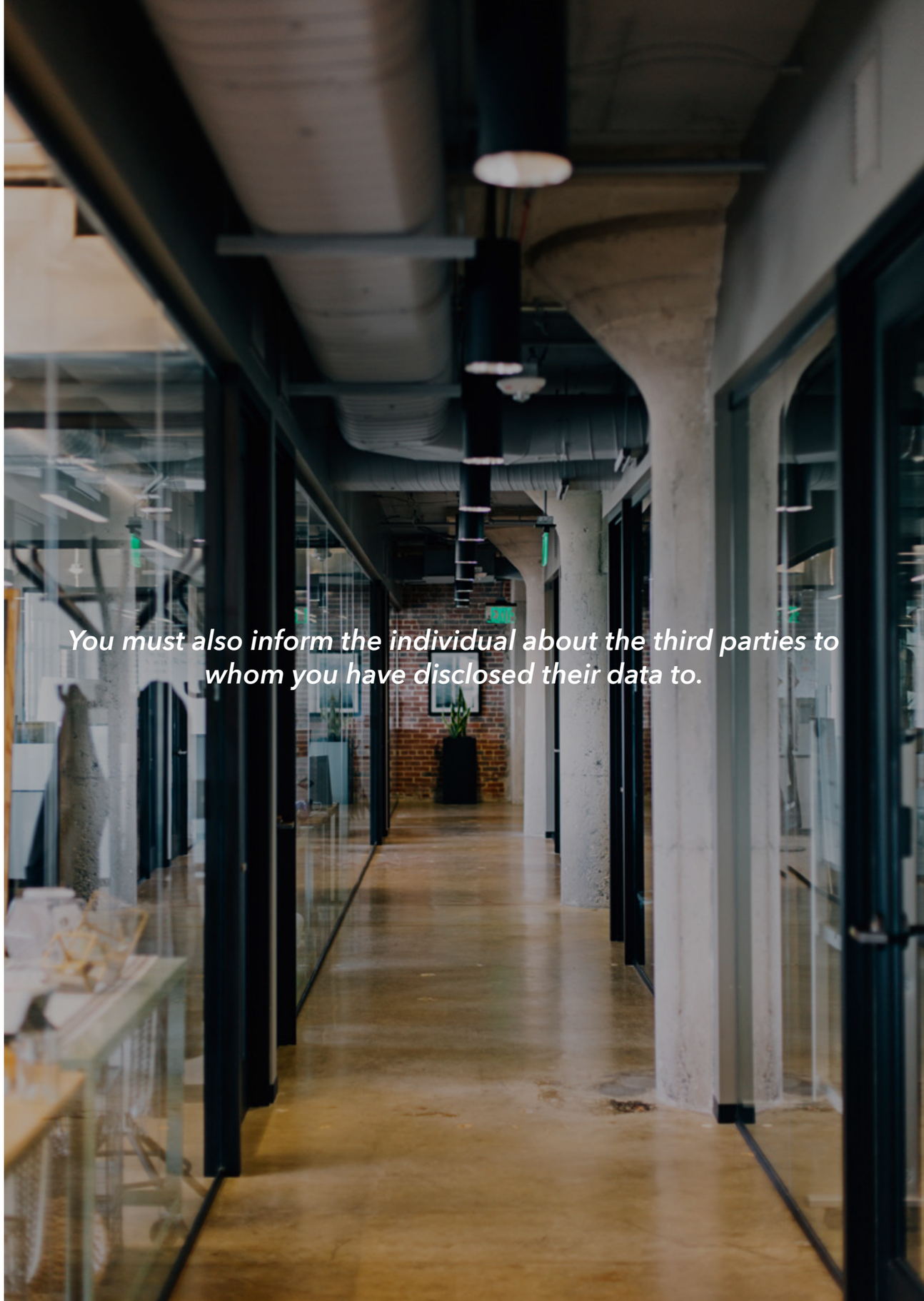
What does this mean?

Individuals can have their personal data rectified if it is incomplete or inaccurate. If the personal data in question has been disclosed to third parties, you must inform them of the amendments where possible. You must also inform the individual about any third parties you have disclosed their data to.

How does Force24 help?

The Force24 platform allows you to update any contact data held at record level in a safe and secure way. All changes take effect immediately.

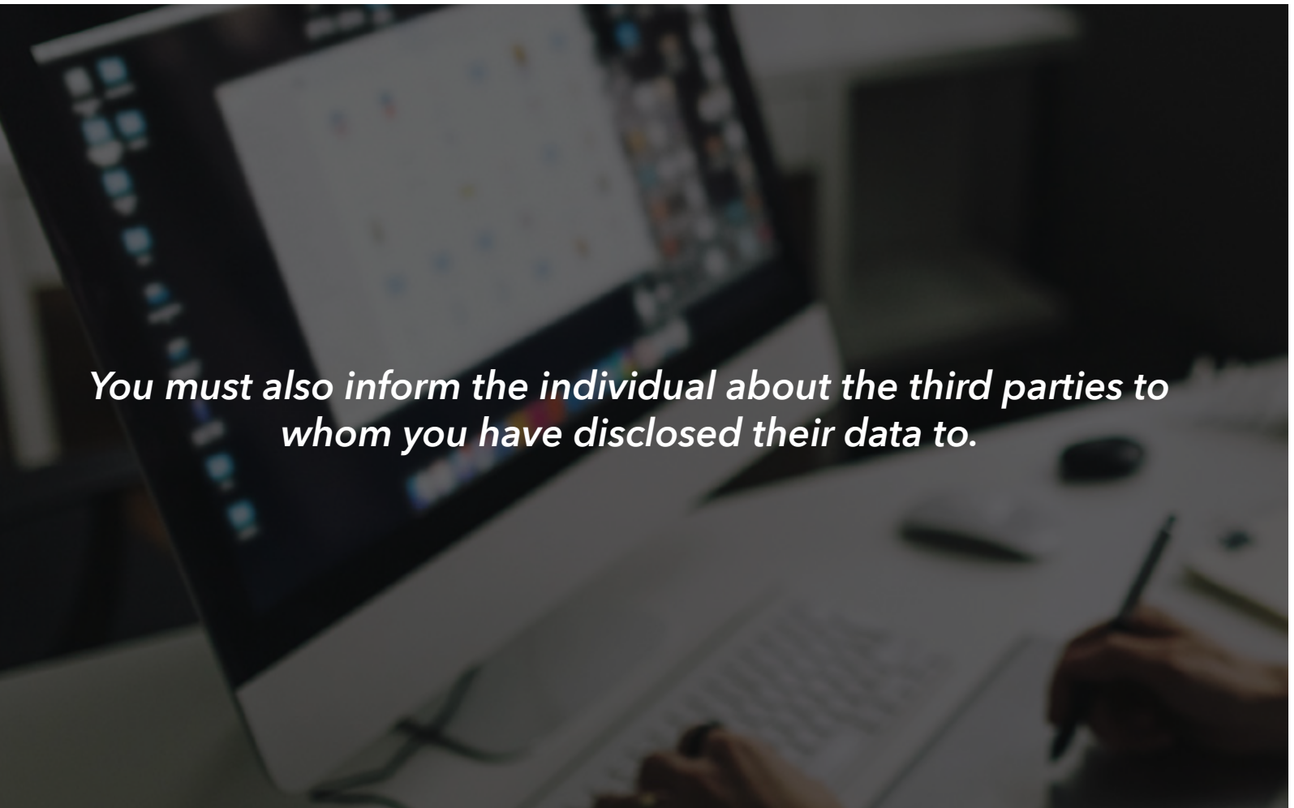
PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access.



The Right To Erasure
(Or Be Forgotten)

What Does This Mean?

Under GDPR, every individual has what is called the "right to be forgotten". This means that people can request that all the data you hold on them is permanently deleted. You will have to ensure that you have a process that easily allows this request and that you remove all the data you hold on that specific individual, across the whole of your business, not just your automation platform. This means you will also need to look at how your data is stored and shared across your business so that you can be confident it has been deleted from every place it is held. It is your right to reject an individual's right to be forgotten, however you must have good reason to do so.



However, the issue with the right to be forgotten is you still need a method of remembering you have forgotten the individual, so some record is still needed!

How Does Force24 Help?

Within the Force24 platform each individual has multi-dimensional permissioning, which enables you to set appropriate contact status for email, direct mail and SMS and, in addition to channel permission, an overall contact status setting will allow:

Active
Full data processing, active for marketing (subject to channel permissions)

Inactive
The individual is disabled. The contact's data will not be processed or interrogated in anyway but held in the secure data environment. No email or SMS can be sent to individuals in this state.

Removed
The individuals and all associated information has been removed. To ensure Force24 does not allow contact in the future, a 256bit encrypted hash of their email address is stored to ensure the contact cannot be recreated at a later date by accident.

All activity collected by the Force24 platform associated with a removed individual will be made obfuscated and maintained for statistical purposes only, within your account.

This setting cannot be overruled. To rectify any mistakes or activate any previously erased contacts, you must address a letter to the Force24 Head of Data Processing to state your reason.

PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access.

The Right To Restrict Processing

What does this mean?

This is an individual's right to suppression of their personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. This applies when:

- An individual contests the accuracy of their data, and it must be restricted until this has been verified.
- An individual objects to processing, and you are considering the request.
- An individual does not want data to be erased when processing has been unlawful and would prefer it to be restricted.
- Your organisation no longer needs the data, but the individual requires the data to defend or exercise a legal claim.

How does Force24 help?

As with the right to erasure, the right to restrict processing is achieved by the use of the multi-dimensional permissioning aspect of the Force24 platform.

By using the Contact Status Inactive, you can assure the user that they will be held in a non-processed state. This setting can be overruled by an authenticated user within the Force24 platform.

PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access.



The Right To Data Portability

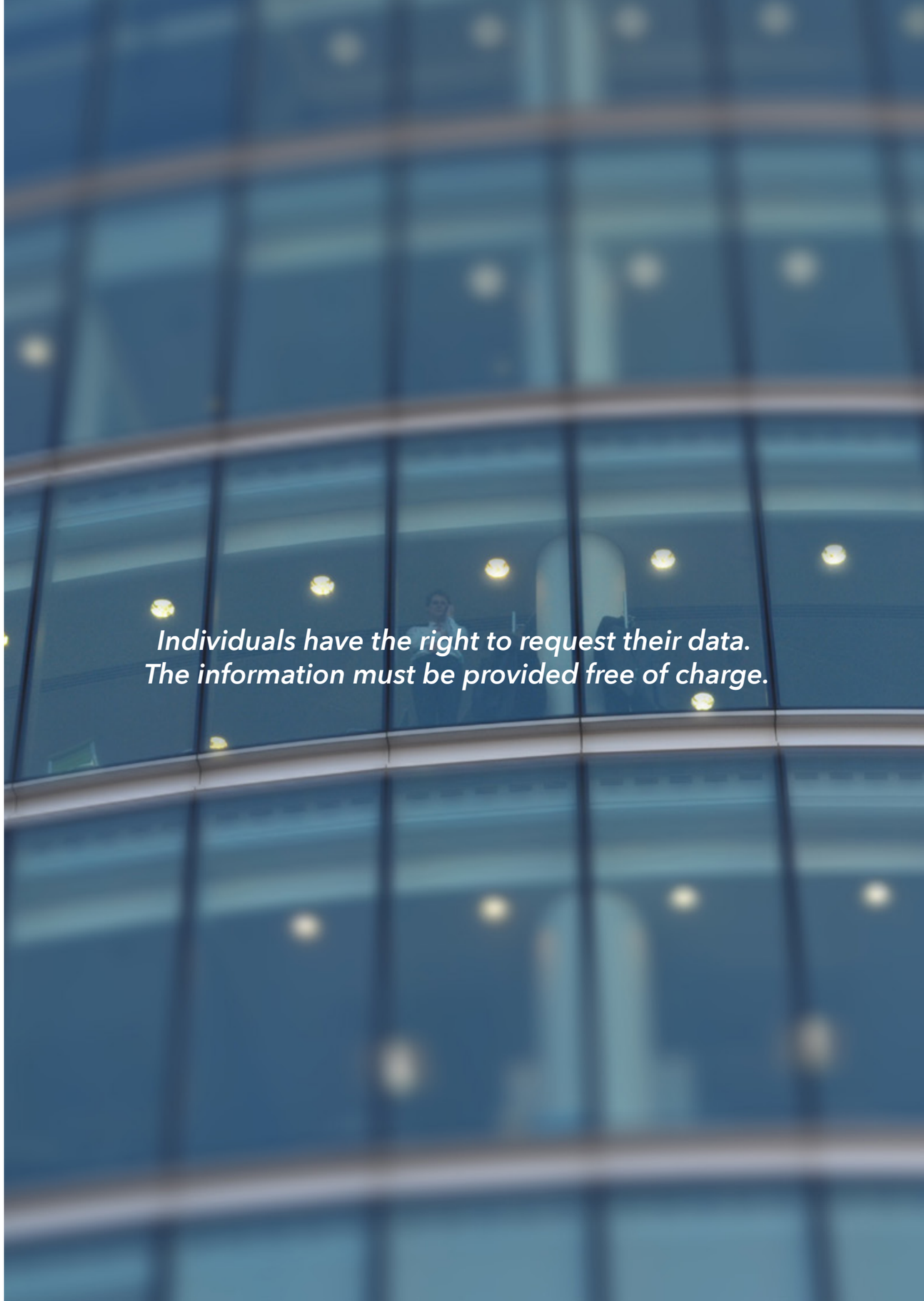
What does this mean?

Under GDPR, individuals also have the right to data portability, meaning they can request their data in a readable, electronic format in order to reuse it across different services. The information must be provided free of charge.

How does Force24 help?

Force24 has implemented a free to access report detailing all information held on any individual contact. The report may be requested at any time and will be delivered within two working days of your request. The report will then be transmitted via a protected XLSX file for your onward transit to the necessary recipient.

PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access.



The Right To Object

What does this mean?

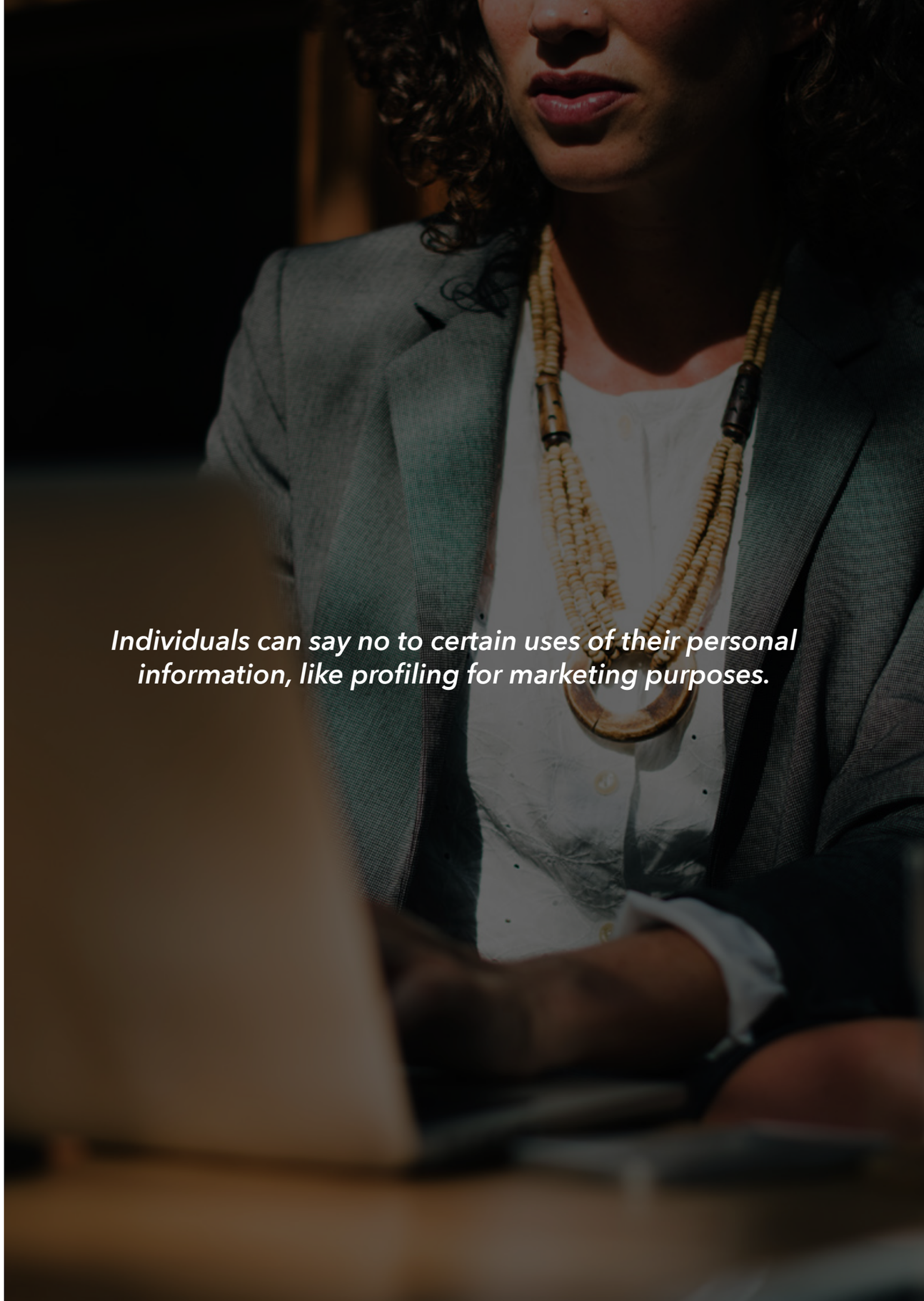
Individuals can say no to certain uses of their personal information, like profiling for marketing purposes. This means if you have lawfully collected data from a group of customers and then want to use that data analytically to look at shopping habits and create sales personas, for example, an individual may request you stop processing their data.

How does Force24 help?

If you have not included ‘profiling’ in your original consent statement, it is advisable that you implement within your Privacy Statement information advising on how to object to processing.

Since you will have no grounds to refuse, or for exemptions, you must comply with the individual’s request. Through using the Contact “Inactive” Status, it will cease to process the contact any further. Please note since profiling is no longer possible, the individual must forfeit the right to subsequently receive marketing messages..

PLEASE NOTE: Your obligations under GDPR will extend far further than just the marketing remit. It will therefore be necessary to ensure that other departments such as accounts and HR have addressed the right of access.

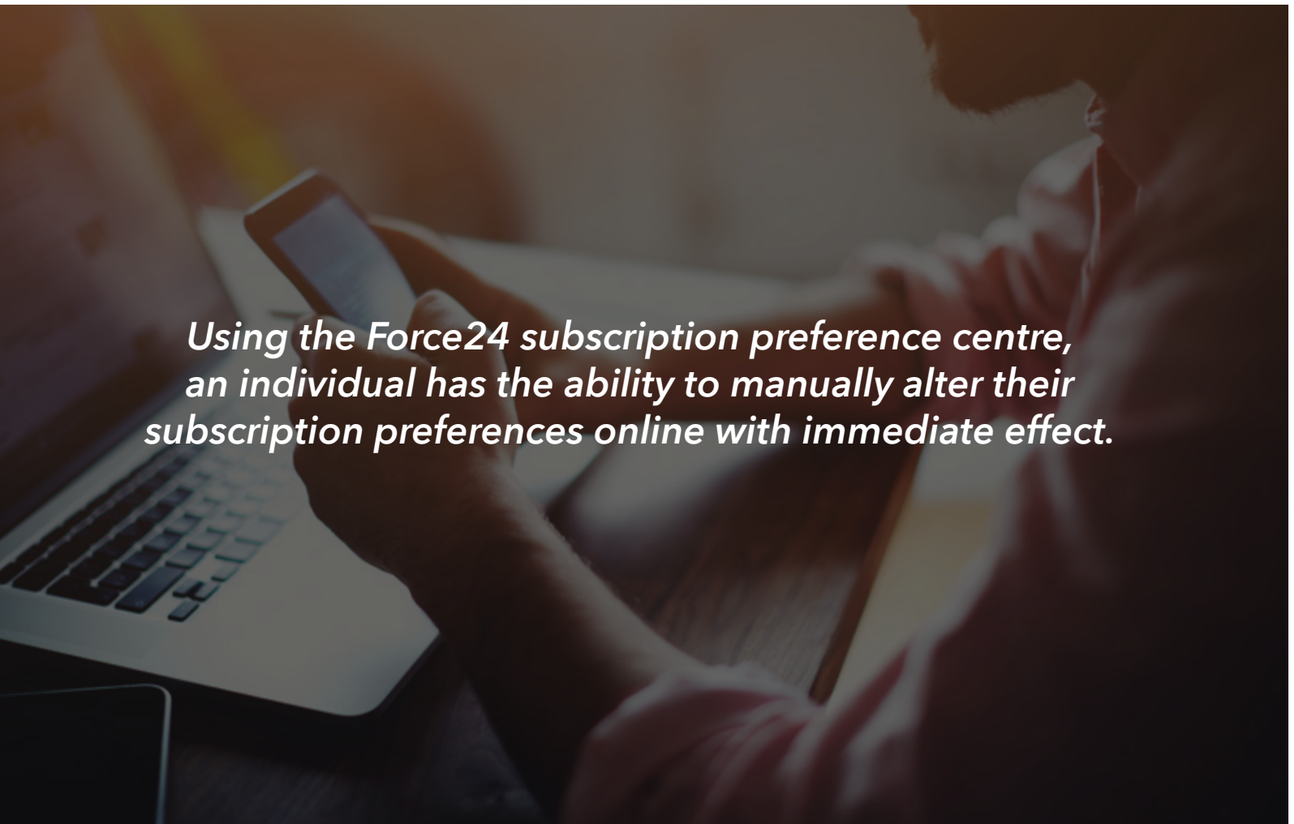


Rights In Relation To Automatic Decision Making And Profiling

What does this mean?

Individuals have the right not to be subject to a decision when it is based on automated processing, such as when a bank uses this process to decline a credit card. The individual must be able to obtain human intervention, be able to express their point of view and be able to obtain an explanation of the decision and challenge it.

Profiling is defined as automated processing intended to evaluate certain aspects of the individual such as work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.





How does Force24 help?

All decisions made within the Force24 platform follow clear rules implemented by the authorised user of the platform. All decisions are revocable and can be subject to human intervention. Organisations should ensure they have a suitable process for individuals to appeal against automated decisions made, relating to their marketing preferences. Using the Force24 Subscription Preference Centre, an individual has the ability to manually alter their subscription preferences online with immediate effect.

All Data Controllers and Processors need a valid legal basis for processing data. GDPR provides six options for processing. These comprise: consent, contract, legal obligation, vital interests, public task and legitimate interests. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Force24 believes your legal basis for processing data will normally fit into two categories comprising legitimate interests, or where contractual relationships exist, to meet your contractual obligations. It should be noted that neither legitimate interests or contractual obligations can override the rights of the data subject and any attempt to do so would be in breach of GDPR. Where questions concerning processing need to be addressed, Force24 will arrange for you to speak to its Data Protection Officer.

Definitions, Legal Notes And GDPR Support

Information Commissioner's Office (ICO)

The ICO is responsible for managing GDPR and after May 25 2018, there is a mandatory requirement to report any data breaches to the organisation, which has the right to investigate and issue fines.

Controller

GDPR defines the Controller of the data as the business or organisation that determines alone or jointly with others the purposes and means of the processing of personal data.

Processor

The Processor is defined as the business, public authority, agency or other body which processes personal data on behalf of the Controller such as Force24, a payroll company or research firm.

For the purposes of providing its marketing platforms, Force24 is acting in the capacity of data Processor under the instructions and guidance of the client, who is the Data Controller.

Accountability

It is the Controller's responsibility to keep appraised of data protection under GDPR as ultimately the data controller is accountable to the ICO for ensuring that all processes implemented by the organisation are in line with its obligations under GDPR. With effect from May 25 2018, both the Controller and Processor will be jointly and severally liable for any data breaches.

Personal Data

Personal data is anything that can identify a 'natural person' and can include information such as a name, a photo, an email address (including work email address), bank details, posts on social networking websites, medical information or even an IP address.

More information

Further information concerning GDPR can be found on the ICO's website: https://ico.org.uk/

Help and Support

Force24 has formed a strategic alliance with Allott and Associates to provide simple solutions to help you navigate through the GDPR compliance minefield. Services include GDPR audits, workplace training, GDPR compliant document drafting and mentoring. To organise a full GDPR audit for your business please visit:

http://landing.force24.co.uk/gdpr-deadline/

Get In Touch

For information on other services like training, please email: philip@force24.co.uk

About Force24

Force24 is a world-class, UK-built, cloud-based marketing automation solution used by enterprise clients and niche SMEs alike. Trusted by leading brands such as WorldPay, Aviva & npower, the intuitive platform empowers marketers to generate faster, more efficient & meaningful conversations with customers & prospects. The result? Increased conversions, revenue & campaign ROI.

In fact, thanks to 8 million data triggers & the expertise of Force24's in-house marketing pros, the platform helps generate £50m revenue for clients each month!

What's more, the Fore24 team isn't just made up of tech gurus and marketing pros. We even have our own in-house GDPR expert to ease every concern and ensure clients are fully regulation-ready!

Get in touch

For further information please visit **www.force24.co.uk** or call **0845 272 5990**. Alternatively, to drop us a line or sign up for our upcoming webinars, email **info@force24.co.uk**

Force24™
Marketing Automation

Force24 Ltd, Office 2, Indigo Blu, 14 Crown Point Road, Leeds, LS10 1EL – Tel: 0845 272 5990 – info@force24.co.uk