GDPR | What does it mean for your business?

The General Data Protection Regulation ("GDPR") is intended to bring European data protection and privacy laws into harmony and into the 21st century by building on the existing laws and concepts.

In this GDPR white paper, we summarise the key points in the regulations, provide our thoughts on the new regulations and explain the development work we have implemented to support your organisation with its GDPR compliance ahead of the 25th May 2018 deadline.

This document is intended purely as an aid and does not cover every point in the General Data Protection Regulations. We therefore recommend that you consult with a GDPR specialist to ensure that your business conforms to the requirements of these new regulations.

Definitions	
Personal Data	The definition of personal data has been widened under GDPR. Personal Data includes information which identifies an individual, and now also information which makes an individual identifiable. This could include IP addresses and online data sets that when taken together can reveal a detailed profile of an individual.
Processing	Processing is defined so broadly in the GDPR as to cover anything that can be done with data, including storing or deleting it.
Data Controller	Article 4 of the GDPR defines a Data Controller as a person (either a natural person or a company) who, alone or jointly with others, determines the purpose and means of the processing of personal data. You determine how and why the personal data of your customers is processed, and are therefore a Controller for the purposes of the current data protection laws, and GDPR.
Data Processor	A Data Processor is defined as a person who processes personal data on behalf of the controller. In the case of Influence Cloud Direct and Influence Cloud Desktop, Influence Limited acts solely as a processor in relation to any data processed by an Influence product; we process data on behalf of you, our customers. In the case of Influence OnSite, Influence is not a Data Processor or Data Controller and there are no obligations for Influence under GDPR.

Your Responsibilities as a Data Controller

Under Article 5 from the EU GDPR, the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data and where necessary, you will also need to implement appropriate data protection policies. Although not an exhaustive list, the key principles include:

Lawfulness

GDPR provides that processing is lawful if it is carried out on one or more specified grounds. For the majority of Influence Limited's customers, three of the specified grounds will be relevant. These are:

1. **Consent |** Consent is the grounds of processing which gets the most press coverage, and is an absolute requirement for marketing, but will typically not be the ground on which most processing relies. Consent must be fully informed and unambiguous, and can be withdrawn at any moment; in the case of withdrawal of consent to processing, all future processing based on that consent must immediately cease.

2. **Necessary for the performance of a contract |** Here your grounds for processing are distinct from consent; for example, you may process a candidate's cv under their instructions in order to find a suitable role for them at a client , but that same candidate may not have provided you with consent to market to them.

3. **Necessary for the legitimate interests pursued by the Controller, except where overridden by the fundamental rights of the data subject |** These are the widest and most useful grounds for processing under GDPR, and allows Controllers to carry out processing activities provided that they have given the appropriate weight to the rights of the data subjects concerned. The data subject has a right to object to processing under this ground, at which point the Controller must justify the interests in processing the data.

It is important to note that your Influence Recruitment solution processes personal data for a number of different purposes; the removal of one ground for processing the data (for example, the customer no longer wishes to receive marketing communications) does not mean that processing based on other grounds must also cease.

Processing of personal data shall not reveal information, such as racial or ethnic origin, political opinions, data concerning health, etc. except where the data subject has given explicit consent for the processing of their data for a specified purpose.

Influence Commentary | Marketing Consent

Influence allows you to record the data subject's consent for marketing communications by SMS, email, post or phone. This is currently by use of the Mailshot flag on a contact record (both candidate and client contact), or by use of Key Codes to denote that a candidate or contact has given consent (this enables you to set more than one category). The journal system also enables you to record communications. When a new candidate is added to the system via drag and drop there is a parameter that allows you to automatically generate a registration email to the candidate. You could of course use this to send links to your privacy policy, send terms and conditions and request opt in to marketing campaigns.

Influence New Development | Policy Management

RELEASED - 1.00.17.339
Influence has developed a brand new *Policy Management System*. This will enable you to store the text of your privacy policy, terms and conditions and any other relevant processing documentation. The policy system will enable you to set candidates and contacts against those policies. You will then be able to track who has opted in, who has opted out and who you have not heard from. The *Policy Management System* will also enable you to trace the date and method that consent was received (or withdrawn) and exactly which policies they agreed (or disagreed) to at the time. You will be able to make policy revisions which will allow you to track who is on an older version of a policy and needs to be given updated policy information.

For more information, please see: Policy Management

Fairness and Transparency

Fairness and transparency means that you are obliged to tell your customers and candidates how you are processing their data, and who it is being shared with (for example you will send candidate personal information to customers in order to decide suitability for interview).

One of the purposes of GDPR is to create transparency in processing chains for data subjects, who should be able to follow their data and exercise their rights against anyone processing that data.

It is worth noting that similar provisions apply where you receive personal information indirectly (e.g. through job boards).

Influence Commentary

The key to compliance with the fairness and transparency principle will be the privacy statement that you provide to your customers and candidates, and which we anticipate will set out the information required under GDPR.

Influence New Development | Policy Groups

RELEASED - 1.00.17.339
The new *Policy Management System* will enable you to store the text and publication date of your policies. You will be able to assign candidates and contacts to these policies, and track who has opted in and opted out. In the case of your privacy policy, this will include a statement of your data processing policies if the content of your policy changes, we can track who read and agreed to the previous privacy notice. We can then send an email to each of these detailing the amended policy text and requesting permission. This is Managed using Policy Groups - Groups of Candidates or Contacts linked to Published Data Policies

For more information, please see: Policy Groups

Personal Data must be Adequate and Relevant

All Data processed must be:

1. **Adequate and Relevant |** Personal Data held should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

2. **Not be kept for longer than required |** The principle that data should be adequate and relevant means that you should not be keeping data for longer than it is required, or hold more data than you require for the specified purposes for which you are processing it. You need to be able to identify customer data for which the storage is no longer necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods where it will be solely used for archiving purposes for a number of reasons, as listed in the General Data Protection Regulations.

3. **Up to date and Accurate |** Any data that is being processed must be up to date and accurate.

Influence Commentary

Existing search tools allows you to search for and communicate with candidates, contacts and clients who have had no activity for a specified period of time. Similarly, you can search for candidates who have contact information over a certain age. These tools can be used to send emails to candidates and contacts requesting updated information and consent.

Influence Development | Removal Tools

IN PROGRESS
An analysis has been undertaken to identify all the tables within Influence where personal information is stored. As a result of this investigation we have updated some of our removal tools in order to make removal of data easier and more transparent to the end user. There is still a degree of manual removal required in order to remove a candidate or contact's personal data. Further updates to these removal tools will come soon.

We have also introduced the Data Protection Manager

For more information please see, Data Protection Manager

Secure

The Controller must have in place systems and processes that protect the confidentiality of personal data.

Data protection by design and by default
Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Influence Commentary

Within Influence, there are already a number of security measures in place, including:

- User permissions – allowing you to lock down who can access and edit a data subject's personal data.
- Password control on your Influence database.
- Password controlled restrictions on data export.
- Data Security processes and procedures within our data centres for Influence Cloud Direct and Influence Cloud Desktop. All hosting partners are ISO 27001 certified.
- Influence Cloud Desktop runs inside your cloud desktop which is accessed through an encrypted remote desktop connection.
- Influence Cloud Direct is accessed over a TLS/SSL connection and all traffic to and from the Influence Cloud Direct server is encrypted in transit.

Our Responsibilities as a Data Processor

Influence are Data Processors for Influence Cloud Direct and Influence Cloud Desktop only. For OnSite installations of Influence, you are both Data Controller and Data Processor.

Under GDPR, Data Processors have the following obligations:

To Meet the Requirements of GDPR

Processing must meet the requirements of GDPR and data must be processed in accordance with the Controller's instructions

Influence Commentary

Data security is at the heart of everything we do. Our hosting partners are all ISO 27001 certified. Our hosting partners operate out of UK Data Centres only. We are bound by detailed security policies, with many stringent data security strategies in place for both Influence Cloud Direct and Cloud Desktop. See Appendix A for more information.

Sub-contracting of Data Processing

Sub-contracting of data processing must be with the consent of the Controller.

Influence Commentary

Influence subcontracts hosting to our hosting partners as follows: For Influence Cloud Desktop, we use Cloud Direct (On Direct Business Services Limited) and for Influence Cloud Direct we use Virtual Tin Limited to host our network infrastructure and servers. Both hold ISO 27001 certification and have incredibly resilient security systems in place. We do not sub-contract processing to anyone else that you do not have a direct contract with. We will inform you of any new sub processors should they be appointed.

Contracts

A binding contract must be in place between Controller and Processor

Influence Commentary

All customers sign a binding contract with Influence. The terms of our contract will be revised to reflect some specific points in the GDPR regulations. Our website reflects the present terms and conditions for our Influence services along with our Privacy Policy.

Demonstrate Compliance

Processors must demonstrate compliance by maintaining a record of all categories of processing activities, details of the controllers and any other processors and of any relevant Data Protection Officers (DPOs), the categories of processing carried out, details of any transfers to third countries and a general description of technical and organisational security measures.

Influence Commentary

Influence maintains a register of all Data Controllers using our services (our customers). Influence also maintains records of the categories of processing activities and the details of our sub-processor data protection officers at On Direct Business Services Limited and Virtual Tin. We have stringent security measures, with detailed security policies in place.

To Implement Appropriate Security Measures

Processors, like controllers, are required to implement security measures appropriate to the risk. What is appropriate is assessed in terms of a variety of factors including the sensitivity of the data, the risks to individuals associated with any security breach, technical restrictions, the costs of implementation and the nature of the processing.

Influence Commentary

All connections to the services are encrypted (be it via Remote Desktop Encryption for Influence Cloud Desktop or TLS/ SSL connection for Influence Cloud Direct. Each service has a high level of threat protection, attack prevention and security monitoring.. See Appendix A for more information

Notification of Breach

The processor must notify the relevant controller of any data breach without undue delay on becoming aware of the breach.

Influence Commentary

As part of ISO 27001 Influence and its sub-processors have procedures in place to investigate, analyse and report on any suspected security breaches, including notification to the Data Controller and appropriate authorities.

The Individual's Rights

The Right To be Informed

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this. Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓
When should information be provided?	At the time the data is obtained.	Within a reasonable period of having obtained the data (within one month) If the data is used to communicate with the individual, at the latest, when the first

		communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

Influence Commentary

The key to compliance with the fairness and transparency principle will be the privacy statement that you provide to your customers and candidates, and which we anticipate will set out the information required under GDPR. This privacy policy will now require an active acknowledgement and agreement. You will need to provide active opt-ins to agree to processing of a data subject's personal data when you capture that personal data. For existing data you will need to request permission as soon as you can. You can record consent in your current key coding system, and can use this to restrict searches, or to remove personal data. The onus here is on you, the Data Controller, to update your privacy statements to reflect the requirements outlined above.

Influence Development | Data Policy Manager (Padlock)

RELEASED - 1.00.17.339
The new Data Policy *Manager* will enable you to record opt in to different policies and how these opt-ins were received (email, telephone call, trade show). Candidates and contacts can be automatically assigned to a policy or can be manually added to a policy. Should you change your policy you can track the date of opt in and can send an update to all candidates or contacts who opted in to a different policy in the past.

For more, information please see: Data Protection Manager

The Right of Access (SAR)

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

Influence Development | Contact and Candidate Reports

RELEASED - 1.00.17.339
Influence have added a Data Statement (SAR) feature within the *Data Policy Manager* (Padlock). This allows all the current data for a given candidate or contact that is currently being held in the database to be Viewed or a CSV file created. This can then be emailed to the Candidate or Contact to complete the Right of Access.

For more, information please see: Data Protection Manager

The Right To Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

Influence Commentary

The personal data is held within the database and is easily rectified on demand. In general the only data within the database that would be transferred to a third party would the candidate personal data which you have sent to your clients as part of their job processing. It is very easy within the database to list all the clients to which candidate information has been sent if you are using the matching system, and you can inform them of any changes where that data is inaccurate. Please contact your GDPR specialists for more information.

The Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Influence Commentary

The personal data is held within the database and can be deleted on demand. There are however some procedures that need to be undertaken in order to remove all data. For example you must remove documents from a candidate's folder prior to deleting the candidate in order to remove all those files. It is unfortunately very difficult to make this anything other than a manual process as these folders could contain information sent to clients, or important documents relating to contracts that you would not want to remove. The retention of such information may well be required for legal or regulatory purposes even if the candidate or contact wished for their data to be removed. This is an area where we suggest you get advice from your own GDPR and data protection specialists.

Third parties to whom the personal data may have been sent can be tracked using the document transaction system. This feature records every document sent through the system and to who they have been sent so it is a quick process to identify those third parties who need to be informed.

Influence Commentary | **Backup Retention**

Influence Cloud Direct and Influence Cloud Desktop have a 30 day retention period on data. Should a candidate or contact wish for their data to be removed, you will need to make them aware that their information will be stored on backup for up to 30 days after removal from the database.

Influence Development | **Improved Consolidation Tools**

RELEASED - 1.00.17.339

Deleting Candidates and Contacts

Our Delete tool has been updated to with an optional feature which can delete the Candidate's or Contact's document folder when their record is removed from the Database. We are continuing to work on the deletion tools in order to remove further linked records.

Regulatory and Legal requirements may require some or all of this data to be retained regardless of GDPR requirements. Therefore we recommend that you review this prior to deleting any candidate, as the process of removing the primary candidate record will remove most linked records immediately.

Remove Personal Data
As a less destructive method for removal of personal data, we have also added a Remove Personal Data feature within the *Data Policy Manager* (Padlock) for a candidate and client record. This allows a Candidate or Contact record data to be stripped out leaving just the name, and files in the document folder can be individually deleted - please note that this is not a full data removal tool, but will remove the primary source of personal data for that Candidate or Contact. Personal data can, of course, be included in a match record notes, placement details, tasks and journals. Due to legal and regulatory requirements it is impossible to put in place automated rules to decide which of these can or cannot be removed so they will continue to be a manual removal exercise. An administrative user can review and remove those linked records manually.

We will in due course update our Data Policy Manager tool further to allow easier review and removal of some of these linked records.

For more, information please see: Data Protection Manager

Influence Development | Informing third parties

IN PROGRESS
We are developing a new feature in the data protection manager (padlock) in order to allow a user to send a templated request to all third parties to whom personal documentation has been sent in order to request removal of the subject's personal data. This will make it a quicker process to inform those third parties of the data subject request for removal.

The Right to Restrict Processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

Influence Commentary

The personal data is held within the database and can be categorised as appropriate in order to remove from processing. We would expect that in most cases you would remove the appropriate data unless there is a legitimate business reason to continue storing the data (See Right to Erasure above)

The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Influence Development | Candidate and Contact Export

RELEASED - 1.00.17.339
Influence have added within the *Data Policy Manager* the ability to create a pure text or CSV file of all the data being held. This produces a consolidated report that can be emailed to the Candidate or Contact.

For more, information please see: Data Protection Manager

The Right to Object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Influence Commentary
The mailshot flag and key codes can be used to restrict processing.

Automated Decision Making and Profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Influence Commentary
This is particularly relevant for the screening and selection of candidates for relevant jobs. We anticipate that your privacy policy will include details of your profiling activities as part of the job management process.

Appendix A

Influence Cloud Security

Hosting Partners

On Direct Business Services Limited (Thinhost)	
Services Provided	Influence Cloud Desktop
Website	www.clouddirect.net
Certification	ISO 27001:2013 and ISO 20000

In recognition of Cloud Direct's commitment to global standards for security best practice, the packaged cloud provider was one of the first UK businesses to be awarded ISO 27001:2013 certification, in March 2015.

ISO 27001:2013 is the latest international standard and benchmark for information security management. The certification demonstrates that Cloud Direct has implemented and upholds an independently assessed and certified information security management system (ISMS).

The certification proves to customers, suppliers and stakeholders that Cloud Direct is committed to, and compliant with, global best practice for information security. It also proves that Cloud Direct can support its customers' obligations under the Data Protection Act (DPA) 1998 and GDPR (due in June 2018). Cloud Direct has robust policies around access control, incident management, business continuity, physical security, human resources and technical procedures.

On Direct provide Influence Cloud Direct on infrastructure provided by VirtualTin Limited (see below)

VirtualTin Limited	
Services Provided	Influence Cloud Direct, Influence Cloud Desktop (via On Direct Business Services)
Website	www.virtualtin.com
Certification	ISO 27001:2013

Virtual Tin deliver services to On Direct Business Services Limited (Thinhost Infrastructure) and to Influence Limited directly (Influence Cloud Direct services). Virtual Tin are ISO27001:2013 certified and deliver all services from ISO27001 certified data centres including Thinhost Cloud Desktop services and Influence Cloud Direct services hosting.

Service Security Profile

Influence Cloud Desktop and Influence Cloud Direct

VirtualTin / Thinhost services carry high levels of security to Tier III level including facilities, power, cooling, connectivity and all equipment providing the service.

Monitoring technologies offering live information and alerting is in place to monitor all tiers of the service availability.

Capacity planning and delivery technologies allow for huge increases of traffic in event of attack scenarios.

Network Security

Some of the examples of the technologies in use include:

Technology	Protection	Cloud Direct	Cloud Desktop
Firewall	• Gateway Antivirus • Access rules • Intrusion protection • Log monitoring • Geo-location protection • BotNet protection • Reputation defence • DDOS attack protection • Denial of service protection.	✓	✓
Antivirus and AntiSpam	• Data back checking and data protection. • Antivirus and Antispam protection for email for Thinhost provided email services		✓

Hosted Desktop Security	• Group policy to enforce consistency across servers.
	• Service Account password change policies are in place
	• Active directory:
	  ○ ACL security on access limiting users to only access the relevant applications, servers, service and data.
	  ○ Security Groups and User Group level access to services (servers), applications and data
	• Shared platform sniffing employed to stop installation or running of malware tools.
	• Proxies deny access to malicious sites and file types.
			✓

Data encryption	• Hosted Desktops run in a secure encrypted hosted desktop client. • Cloud Direct traffic is TLS/SSL encrypted from Client to Server.	✓	✓
Hosted Desktop Web Security	For Thinhost provided subscribed web browsing services • Internet proxy services • Web filtering technology • Monitoring and Alerts		✓
Logs and Monitoring (there are many but here are just a few)	• Back checking intrusion attempt • Failed log on attempts • Spot check analysis on failed attempts to access on items such as RDS services • Live information and alerting for all tiers of service availability	✓	✓
Data Retention Cloud Desktop	On Direct Business Services (Thinhost) have processes in place to remove customer data for individuals and companies who no longer are customers within their infrastructure in regards to mailboxes, file data, servers and backup retention. After service closure, data is backed up for 30 days and then removed completely. Email - Mailbox is deleted and backup data is retained for 30 days (although requests for restore must be within 14 days). Thinhost will backup your mailbox on request separately to your group drive. Desktop and User Home Drives - when a user is deleted, backup of the user data is available for up to 30 days (although requests for restore must be within 14 days). Thinhost will separately backup the user home drive data on request separately to your group drive. Influence Database Data Retention. After service closure Influence retain your company Influence data for 14 days. The data will then be removed in it's entirety. The backup of this data will then be available for a further 30 days (although requests for restore must be within 14 days)		✓
Data Retention Cloud Direct	Influence Database Data Retention. After service closure Influence retain your company	✓	

	Influence data for 14 days. The data will then be removed in it's entirety. The backup of this data will then be available for a further 30 days (although requests for restore must be within 14 days)		
Data Backup	• All Servers backed up using Systems Centre Data Protection Manager • All servers are backed up at Virtual Server level and file level on overnight backup	✓	✓

Influence Cloud Direct | **Additional Security Information**

Servers are open to the public internet on one port only for the direct connection of the kcml client. All traffic between client and server through this port is encrypted with TLS 1.2 SSL with AES 128,GMC,SHA 156, 128 Bit keys. There is no other open public internet access to these servers. Maintenance and support of the servers is provided using encrypted remote desktop and is restricted to authorised IP address ranges only for the Influence office and selected support staff.

Influence Cloud Desktop | **Additional Security Information**

Influence Cloud Desktop is provided over an encrypted remote desktop connection. The servers storing your Influence data are only open within the closed network accessed by your remote desktop.

Influence Commentary

Please remember that Influence acts only as a data processor. You are required to have your own procedures in place to make sure you are GDPR compliant and to manage and use your data and services appropriately. Usernames and passwords must be treated with the utmost care as a lost or stolen password can lead to serious security vulnerabilities. Please ensure your passwords are changed on a regular basis, both to the services and your login to Influence from within your Cloud Desktop or Cloud Direct connection. All computers accessing the services should be patched to the latest versions of that operating system provided. All computers accessing the services should have up to date anti-virus. We are not responsible for misuse of the system and strongly encourage regular reviews of user database priorities and options to make sure that only authorised staff have access to security sensitive features and functions. Please speak to your systems administrator to make any changes to the database system passwords and priorities. If you have any queries regarding setting up user priorities and Influence system passwords, please speak to the Influence support team who can assist.