GENERAL DATA PROTECTION REGULATION (GDPR)

Vendor Assessment

Date: 01/02/17

Contents

Introduction

We pride ourselves on being a trusted partner of our clients and take security and data protection/privacy very seriously.

In May 2018, a new EU General Data Protection Regulation (GDPR) will come into force which implements a number of obligations for ALL organisations who handle personal data pertaining to EU citizens.

As part of the GDPR, organisations will need to contact their vendors to perform a vendor assessment to ascertain the quality of protection provided.

At Investis, we manage the Corporate and Investor Relations Websites for hundreds of clients and take our role in giving our clients comfort over our quality of protection seriously.

Therefore, in this document, you will find answers to the questions in common GDPR vendor assessment templates.

For the majority of our clients, the only personal data we hold is name and email address of people who subscribe for alerts. There are a few exceptions but this document answers the questions in the context of subscriber information.

Transparency

Are individuals provided with a Privacy Notice explaining the organization's internal Privacy Policy and practices?	When a subscriber signs up to alerts a privacy notice is displayed. The content of the privacy notice is normally provided by the client.
Does the Privacy Notice include the identity of and contact information for the controller or the controller's representative, as well as the contact details of the data protection officer (if any)?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it does include this information.
Does the Privacy Notice describe the types of personal information, including sensitive information, collected from individuals?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it does include this information.
Does the Privacy Notice describe the purposes for which collected personal information, including sensitive information, will be used?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it does include this information.
Does the Privacy Notice describe the circumstances under which personal information is disclosed or shared with third parties, including service providers, and the purpose for those disclosures?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it does include this information.

Does the Privacy Notice include a description of the categories or types of third parties to whom personal information is disclosed or shared?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it does include this information.
Are individuals informed that their personal information will be transferred to a third country or international organization and whether there is a legitimate transfer mechanism in place?	Yes they are.
Does the Privacy Notice describe the method for individuals to exercise choice and update their preferences regarding how their personal information will be used, including whether and to whom it is disclosed?	In the default privacy setup they are but clients configure this but normally they do.
Is the Privacy Notice easily accessible at the time the individual first interacts with the product or service (e.g., accessible via website homepage or app store listing)?	Yes.
Is the Privacy Notice easily distinguishable from other information (e.g., Terms of Service) the organization provides?	Yes.
Is the Privacy Notice written in plain language so that it is easily understood by individuals?	Yes.
Is the Privacy Notice available in all languages in which business is conducted?	Yes.
If the organization seeks consent from individuals for the processing of their personal information within its Privacy Notice, is the request for consent conspicuous and set out from the rest of the text of the Privacy Notice (e.g., bold, highlighted, etc.)?	The Privacy Notice is sometimes provided by Investis and other times by the Client, but it is normally highlighted.
Notice, is the request for consent conspicuous and set out from the rest of the text of the Privacy Notice (e.g., bold, highlighted, etc.)?	It is highlighted and can be prompted as a disclaimer if required.
Is there an immediately visible, clearly labelled, and accessible notice regarding the use of cookies and other passive technologies?	Yes
In the event that individuals are not informed in advance of processing activities, are individuals provided specific information about how their	N/A

information is processed within a reasonable time after the information has been collected and before the information is processed?	

Collection and Purpose Limitation

Is consent obtained from an individual prior to accessing or storing information on their device (e.g., setting cookies)?	Yes
Is an individual's explicit consent obtained prior to collecting sensitive information?	N/A
Are individuals provided a mechanism to change their preferences regarding the use of their personal information?	The data held is minimal but the user can subscribe.
Are individuals able to withdraw consent they previously provided?	Yes, by unsubscribing.
Are an individual's preferences and changes made to those preferences tracked to ensure preferences are honoured on a continuing basis?	N/A
Are an individual's preferences and changes to those preferences communicated to third parties to whom their personal information has been disclosed?	N/A

Quality

Are steps taken to ensure the accuracy and completeness of personal information received directly from an individual or a third party (e.g., edit and validation controls, forced completion of mandatory fields)?	Yes, fields are validated when the subscriber is entering their details.
If it is discovered that information held about an individual is incorrect, is the information promptly deleted or corrected?	Typically, only subscriber information is held. So if emails bounce or are reported as spam then the data is deleted.

Privacy Program Management

Are processes in place to ensure that users, management, and third parties confirm (initially and on an ongoing basis) their understanding of an agreement to comply with the Privacy Policy and procedures related to the security of individuals' personal information?	Yes.
Does the organization maintain documentation regarding the legal basis of cross-border data transfers (e.g., Binding Corporate Rules, Model Contract Clauses, etc.)?	N/A
Are there internal controls in place to ensure that Privacy Impact Assessments (PIAs) are completed on new products or services when information is collected, used, or disclosed in a novel way; when new technologies are in play; or when high risk processing activities are undertaken?	N/A
Do third-party contracts require third parties to process and protect the information entrusted to them in a manner consistent with the organization's policies?	Yes, they do.
Are you a data controller?	The client is the data controller.
Are you a data processor?	Yes

Security for Privacy

Does the organization have a documented security program that details the technical, administrative, and physical safeguards required for personal information?	Yes, we do. We have a full Information Security Management System that is certified to ISO27001 standard.
Is there a documented process for resolving security-related complaints or other issues?	These would follow our normal escalation process.
Is there a designated individual who is responsible for driving remediation plans for security gaps?	Yes, this responsibility falls with the Chief Technical Officer.

Are industry-standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	All data is encrypted at rest and transmitted using https. More information can be found in our Infrastructure and Security document.
Is personal information systematically destroyed, erased, or anonymized when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	If a client leaves Investis then all data is erased.

Data Breach Readiness and Response

Does the organization have a documented privacy and security Incident Response Plan?	Yes, we do.

Individual Rights

Are individuals provided a mechanism to request access to the information held about them so that they may review, correct, and/or update this information?	Yes, The only data held is subscriber information and the subscriber does have access to update this via them either updating their preferences or going to the subscriber page and updating their details.
Are individuals provided confirmation that their personal information has been updated or corrected?	Yes.
Can individuals obtain their personal information that was collected or processed by an automated means in a structured, commonly used, and machine-readable format?	Only minimal data is held and this can be retrieved through a preferences page.
Does the organization provide a mechanism that is clear, conspicuous, and accessible to individuals for privacy-related questions and/or complaints?	Yes.
Are individuals informed of their right to lodge a complaint with a supervisory authority, along with information on how to file such a complaint?	Only if the client logs this in the privacy notice.
Are individuals informed of their right to demand erasure of personal information held about them?	Only if the client logs this in the privacy notice.

Does the organization have controls in place to provide for individuals' right to erasure under the following circumstances?	The client can contact Investis Client Services 24/7 for this to be performed.
Are individuals explicitly informed of their right to opt out of marketing communications and request that their personal information no longer be used for direct marketing purposes?	Data collected is not collected for marketing purposes.
Does the organization make decisions about individuals based solely on an automated processing of their information?	N/A