ITN INTERNATIONAL

Why a white paper on European Union GDPR?

THE WHITE PAPER

GDPR CONSIDERATIONS FOR REGISTRATION/ LEAD RETRIEVAL SERVICES PROCESS

DECEMBER 2017

The new EU General Data Protection Regulation (GDPR) law will take effect May 25, 2018.

The GDPR Event Landscape

Event producers have already begun working on shows for next year, and GDPR compliance will undoubtedly play a significant role in 2018's event planning and execution.

ITN has spent countless hours analyzing the implications of the new law for our industry. While there are many documents out there that deal with this new law, few give specific attention to Registration and Lead Management and how GDPR will affect the vendor responsibility versus the client responsibility in the context of B2B events.

This white paper focuses primarily on events, however it also covers the basic requirements needed for GDPR in a wider context. ITN is actively implementing its GDPR compliance processes and is working with its clients to assist in their compliance activities as well.

ITN believes that this white paper will assist in developing and implementing your own GDPR compliance processes and procedures.

This white paper is provided compliments of ITN International.

For more information, contact our Digital Privacy Officers (DPO):
EMEA: Beverley Honey – bhoney@itnint.com
North America: Chris MacLeod – cmacleod@itnint.com

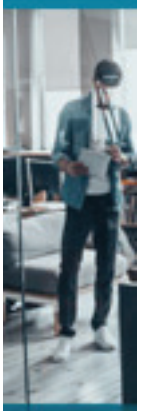
1 Commercial Road, Eastbourne, BN21 3XQ +44 (0)1323 348 8 0 1 www.itnint.com

Introduction

This white paper has been developed to assist participants involved in the Registration and Lead Retrieval Services Process (the "Process"). This refers to the processes and procedures pursuant to which "Registration/Badge Services" and "Lead Retrieval/Follow-up Services" (as those terms are defined below) are obtained and provided in connection with a trade show or convention (an "Event").

Specifically, this white paper provides a high-level summary of (a) the participants in the Process, (b) the General Data Protection Regulation or "GDPR" (Regulation (EU) 2016/679), and (c) the GDPR implications and requirements for those participants. "Registration/Badge Services" refers to registration for an Event by an Event attendee ("Attendee") and the issuance of a badge ("Badge") enabling the Attendee to attend both general and, if applicable, limited access activities during the Event. "Lead Retrieval/Follow-up Services" refers to the process by which an Event exhibitor ("Exhibitor") obtains personally identifiable information or PII of an Attendee for use (a) when the Attendee visit the Exhibitor booth during the Event and (b) post-Event to contact the Attendee to pursue potential business activities.

This white paper is not intended as a substitute for legal advice from qualified legal resources. Recipients of this white paper are encouraged to consult with qualified legal counsel to obtain comprehensive legal advice concerning GDPR compliance. This white paper is intended to provide a high-level description of the GDPR-related issues that can arise in the Process, together with a brief description of the typical steps to be taken to address GDPR compliance.



The Process and the Participants

There are multiple potential participants in the Process, including the producer of the Event ("Event Producer"), Event Sponsors, Attendees, Exhibitors and the actual provider(s) of the Registration/Badge Services and the Lead Retrieval/Follow-up Services (the "Service Provider").

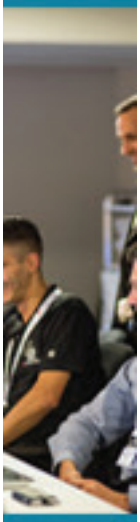
The Event Producer. The Event Producer typically enters into separate contractual arrangements with the Exhibitors, the Attendees and the Service Providers. The arrangement with the Exhibitor focuses on the rules and regulations around space rental, interaction with Event staff and the ancillary services which the Event Producer will make available to the Exhibitor. Particularly relevant to the GDPR, in some circumstances, the Event Producer and the Exhibitor may agree on specific PII to be obtained from Attendees during registration for the Event.

The Attendee. Typically, during registration, the Attendee is required to agree to Event rules and regulations and is asked for consent to share registration information, including PII, for use by the Exhibitors when the Attendee visits the Exhibitor's booth and for post-Event business contacts by the Exhibitor. Generally, the PII is provided to the Exhibitor through scanning of the registration Badge ("Badge") using a software application running ("Lead Scanning Software") on a portable or PC-based scanning device (a "Scanning Device") generally licensed or provided to the Exhibitor by a Service Provider.

The Process and the Participants

The Service Provider. The Service Provider enters into contractual arrangements with the Event Producer and the Exhibitor for the provision of the Registration/Badge Services and the Lead Retrieval/Follow-up Services. The Event Sponsor will usually determine how and what specific PII is to be obtained from the Attendees and how that information is to be shared and used. Generally, the Badge will include embedded information typically found on the Attendee's business card. Importantly, the level and process for obtaining Attendee consent to the use of the PII provided during registration should be included in this agreement. A brief discussion of the GDPR consent requirements is included as Attachment 3 to this white paper. In the agreement between the Exhibitor and the Service Provider, the Service Provider determines how the PII of Attendees is to be obtained and made available to the Exhibitor – generally through the licensing of Lead Scanning Software during the Event. In addition, this agreement describes the process that Exhibitors must go through to obtain access to the PII of Attendees that have visited the Exhibitor booth. This is for use by the Exhibitor to make contact with the Attendee post-Event.

The Exhibitor. As referenced above, the Exhibitor generally enters into separate contractual arrangements with the Event Sponsor and with the Service Provider. The Exhibitor is prohibited from using any PII obtained through use of the Lead Scanning Software for any purpose not described in the Attendee consent and in the contractual arrangements. As indicated above, under certain circumstances and with certain Exhibitors, the Event Sponsor may be willing to consider including PII specifically desired by that Exhibitor in the PII required of Attendees at registration. These circumstances should be described in the Exhibitor/Event Sponsor agreement. In other words, under some circumstances, the Exhibitor may participate in the determination of what PII is to be collected and how it is to be used. This is relevant in determining the status of Exhibitors for GDPR compliance purposes. See discussion of Data Controller below.



The General Data Protection Regulation

The European Parliament and the Council of the European Union have adopted a comprehensive regulation and rulemaking authority aimed at addressing the use or "processing" of "Personal Data" concerning EU citizens or residents ("Data Subjects"). The so called "GDPR" takes full effect on May 25, 2018. Adopted in April 2016, with a two-year lead time prior to enforcement, the GDPR adopts a wide range of requirements governing the use and handling of Personal Data of Data Subjects that will have significant impacts for any company doing business (offering or promoting the sale of goods or services) in any EU member state or which "processes" Personal Data of a Data Subject. For purposes of this white paper, the terms "Data Controller" or "DC" and "Data Processor" or "DP" are particularly relevant. See the discussion of these roles below. For convenience, a high-level checklist of the recommended process an entity should undertake to assist in identifying business activities aimed at helping to ensure GDPR compliance, including a more detailed description of the general GDPR requirements, is set forth in *Attachment 2*.

The General Data Protection Regulation

To what information and what entities does the GDPR apply?

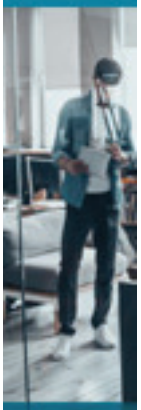
The GDPR applies to any person or entity that determines how and for what purposes Personal Data is to be "processed" (a "Data Controller") and to the entity that actually "processes" Personal Data, (a "Data Processor"). Personal Data is any information concerning an identified or identifiable natural person enabling the identification of such person, directly or indirectly. "Directly or indirectly" refers to the ability to associate the relevant data with a specific individual, by use of other information or data, regardless of source. The GDPR does not apply to data that has been rendered anonymous, provided there is no ability to associate the data with any individual under any circumstances. For example, information about an individual where an anonymous identifier has been adopted, is Personal Data if there is any way to associate the identifier with the individual. The GDPR adopts a fairly strict standard for determining whether information is truly "anonymous." Put more simply, if a given data element can be associated with an individual through any foreseeable process, even if there is no intent to so associate and even though the process may involve the cooperation and provision of information from a third party which has no obligation to so cooperate or provide, the information would likely be treated as Personal Data. "Aggregated" information such as the number of individuals who attend Events from each EU country is not Personal Data as long as there is no ability to identify any one individual included in the aggregated data.

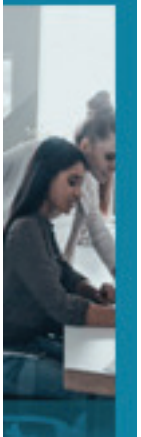
What does "processing" mean?

The GDPR has adopted a very broad definition and for all practical purposes, "processing" means anything that is done to or with Personal Data. Companies should conclude that if they have access to or possession of Personal Data concerning any Data Subject, they are subject to the GDPR. **As a general rule, in the Event context, the GDPR will likely be deemed to apply if any Personal Data of one or more Data Subjects is processed or to be processed or if the processing of any Personal Data is to occur in the EU.**

Is my company a Data Processor, a Data Controller or both?

A Data Controller or DC is the entity that alone, or jointly with others, determines how and for what purposes Personal Data are processed. A Data Processor or DP is the entity that alone, or jointly with others, actually processes the Personal Data. An entity that both determines how and for what purpose Personal Data are to be processed and which actually does the processing is both a Data Controller and a Data Processor. If the entity is acting on behalf of a third party in processing and the third party is the sole determiner of the means and rationale for processing that is performed by the entity, then that first entity is a Data Processor and not a Data Controller. Generally, a vendor that has access to Personal Data on behalf of its customer or client is at least a Data Processor, but may be a Data Controller depending on the terms of the vendor contract.





The General Data Protection Regulation

The GDPR imposes direct obligations on both the Data Controller and the Data Processor. A determination of the specific obligations depends on the specific circumstances for each type of processing. See Attachment 1 to this white paper for a summary of the obligations imposed on Data Controllers and Data Processors. A Data Processor may designate one or more "sub-processors. A "sub-processor" is a vendor of the Data Processor that processes Personal Data on behalf of the Data Processor, and with the consent of the Data Controller. For example, if (a) Company A is the Data Controller, (b) Company B is the Data Processor, and (c) Company B sub-contracts with Company C for the performance of certain processing functions, then Company C is a "sub-processor." The contract between Company B and Company C must cover certain required matters to comply with the GDPR and Company A, the Data Controller, must consent to the use of Company C for "sub-processing."

Broadly speaking, what does the GDPR require?

The requirements of the GPDR can be broken down into several general categories as follows:

Lawful basis for "processing." The burden is on the Data Controller to demonstrate a lawful basis for processing the Personal Data. This includes the requirement that the lawful basis be ongoing, so that once the lawful basis no longer exists, the Personal Data should be deleted. Consent is the most common "lawful" basis for processing.

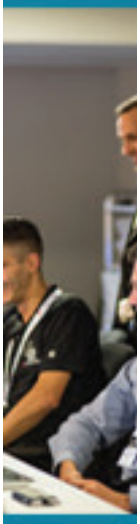
Required consent. The Data Controller must ensure that the Data Subject provides her specific, express and freely given consent for each and every instance of processing of her Personal Data. See Attachment 3 for a summary of the consent requirement.

Rights of inspection, correction and deletion. The Data Controller must ensure that Data Subjects are provided with a readily available process for reviewing their Personal Data which has been collected; a process for correcting any erroneous Personal Data; and the right to require that their Personal Data be deleted (the "right to be forgotten").

Protections and internal procedures. All Data Controllers and Data Processors must have internal processes and procedures in place for the protection and safekeeping of Personal Data which are deemed adequate under the GDPR.

Data security breaches. All Data Controllers and Data Processors must adopt appropriate processes and procedures enabling the timely and appropriate response to any improper access to or processing of Personal Data.

Trans-border Transfers of Personal Data. No Personal Data can be transferred outside of the EU, unless the Data Controller and Data Processor have taken appropriate steps to ensure the proper handling of the Personal Data under the law of the receiving country, by legal contract, adoption of appropriate binding corporate rules or other prescribed means permitting such transfer. For proposed transfers of Personal Data from the EU to the United States, it is possible to utilize the "Privacy Shield" arrangement in place between the EU and the United States.



The Privacy Shield regime is administered by the U.S. Department of Commerce. This requires that a company certify compliance with Privacy Shield requirements, which then have the force of law. As with all GDPR issues, interested businesses should consult with legal counsel for advice on the requirements of the Privacy Shield certification. It is important to note that Privacy Shield certification only addresses cross-border transfer of Personal Data and not the other requirements of the GDPR.

Consequences of non-compliance. Failure to comply with the requirements of the GDPR can result in fines up to 4% of global annual turnover for certain serious infringements and 2% for less serious infringements. See Attachment 4 for further information on potential fines for GDPR non-compliance.

It is important to note that the contract between the Data Controller and the Data Processor contains provisions whereby the Data Controller seeks to ensure that the Data Processor enables the Data Controller to comply with its GDPR obligations.

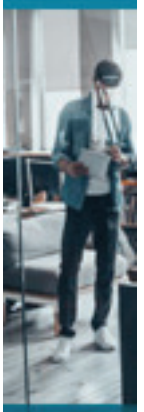
The GDPR and the Process

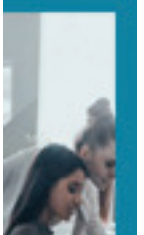
The key to understanding the GDPR obligations of any participant in the Process is a determination as to which participant acts as the Data Controller and which acts as the Data Processor. As previously indicated, this determination will depend on the facts and circumstances of each proposed transaction. Any given business arrangement can involve one or more Data Controllers and one or more Data Processors. A DP can also designate and contract with sub-processors to perform some or all of the processing functions it would otherwise perform, provided that the Data Processor has the Data Controller's consent and the appropriate contractual arrangements exist. The same entity can be both a Data Controller and a Data Processor.

For purposes of this section, the generic description of the roles and contractual relationships of the participants described above are assumed to apply.

The Event Producer. Generally, the Event Producer will be characterized as a Data Controller, since that entity determines what services are to be provided to Exhibitors and Attendees and by whom, what information is to be collected from Attendees and for what purposes. Typically, the Event Producer does not undertake the actual processing of the Personal Data, although it is possible for the Event Producer to be a Data Processor. While all obligations of a DC will apply if the Event Producer is deemed to be a DC, key issues are ensuring that the appropriate Attendee consents are obtained and maintained, that no processing is authorized if such processing is inconsistent with the description contained in the consent and that all Data Processors are contractually obligated to meet their obligations as DPs.

The Attendee. The Attendee will be the Data Subject, provided she is an EU Subject. She must be afforded the right to inspect her Personal Data, to restrict the processing of that information and her knowing and affirmative consent must be obtained for any processing of her Personal Data.



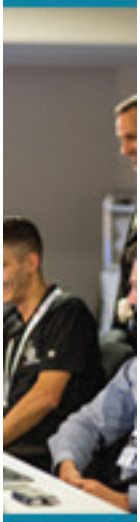


The Exhibitor. Generally, the Exhibitor will be a Data Controller (since the Exhibitor will determine the uses for the contact information obtained by scanning the Badge or by otherwise rightfully accessing the information) and may be deemed a Data Processor to the extent that the Exhibitor uses the Personal Data, but does not determine how all Personal Data in its possession is to be processed. As indicated above, the Exhibitor may be involved with the Event Producer in the determination of what Personal Data is to be collected at Event registration. The Exhibitor may also be involved in the process pursuant to which the roles and responsibilities of the Service Provider are defined. Additionally, the Exhibitor will likely determine exactly how the Personal Data is used for lead retrieval and/or follow-up purposes.

The Service Provider. Typically, the Service Provider will be a Data Processor. In fact, that is the primary function of the Service Provider – to store, transmit and manage the Personal Data and ensure that the Personal Data is processed only in a manner consistent with the consent obtained from the Attendee.

Summary and Conclusions

As summarized in this white paper, extensive affirmative obligations are imposed when an entity is deemed to be a Data Controller or a Data Processor. Each status drives a specified set of obligations which must be met in order to avoid the potential for significant fines. The existence of these obligations should drive an early determination of the status of each participant in a set or series of business transactions that involves the collection, use, transmission or storage of Personal Data. In the event an entity contemplates engaging in any of these activities, qualified legal counsel should be consulted and appropriate contractual relationships should be concluded. This white paper should not be a substitute and is not intended as a substitute for obtaining qualified legal advice. As indicated above, this white paper is intended to provide a high level description of the obligations and issues raised by the GDPR in the context of the Process.



ATTACHMENT 1

GDPR REQUIREMENTS FOR DATA CONTROLLERS AND DATA PROCESSORS

GDPR Obligations of Data Controllers

A DC is the entity that alone or jointly with others, determines how and for what purposes Personal Data are processed. While not exhaustive, the DC has the following primary responsibilities under the GDPR –

The DC must ensure compliance with all GDPR data protection principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation; and
- Integrity and confidentiality

The DC must ensure that its own processing activities are in compliance with the GDPR, including the requirement that there be a "lawful purpose."

The DC must ensure that data privacy principles are built into its product and service development processes.

The DC and any joint controller must allocate the responsibilities for GDPR compliance

The DC must obtain a lawful consent from the Data Subject, authorizing the relevant processing and by which DP. See Attachment 3.

DC must provide access to and an opportunity to delete or correct Personal Data.

DC must maintain written records of all data processing activity which it or its DPs under take.

The DC can appoint Data Processors which must guarantee compliance with the GDPR, including only processing Personal Data as instructed by the DC and ensuring the security of Personal Data that it processes.

The DC must implement appropriate organizational and security measures to protect Personal Data against improper access or use.

GDPR Obligations of Data Processors

The DC must report any data security breaches to the relevant governmental authorities and under certain circumstances, the relevant Data Subjects must also be notified.

If the DC not established in the EU, it must designate an EU-based representative, unless subject to exemption based on frequency of processing. This exemption applies if there is only "occasional" processing of Personal Data, the Personal Data that is processed does not involve particularly sensitive Personal Data and the processing that is undertaken is unlikely to result in a risk to the rights and freedoms of individuals. There is currently no clear guidance on how these exemption requirements will be interpreted.

DC must ensure adequate protection if Personal Data is to be transferred outside of the EU.

A DP is the entity that actually processes Personal Data as determined by the Data Controller. Of course, a single entity can be both a DC and a DP. There can also be multiple DPs f or a given set of business transactions, each of which could designate a sub-processor, with the consent of the DC and with the inclusion of the required contractual protections. While not exhaustive, the DP has the following primary responsibilities under the GDPR:

- DP must assist the Data Controller in the fulfillment of its obligations
- DP not established in EU must designate an EU-based representative, unless exempted based on frequency of processing.
- DP cannot engage a sub-processor without consent of DC, which sub-processor must be subject to the same obligations as the DP.
- DP must have written agreement with DC that defines the scope of the processing and prohibits processing of Personal Data except upon the written instructions of the DC; may include "standard contractual clauses" as a means of meeting obligations.
- DP must maintain written records of processing activities.
- DP must institute appropriate technical and security measures to enable GDPR compliance.
- DP must notify DC of any data security breach.
- DP must comply with cross-border transfer requirements.

ATTACHMENT 2

GENERAL DATA PROTECTION REGULATION OPERATIONAL REQUIREMENTS

Required/Recommended Action	Activity Involved/Comments
Develop and Obtain Buy-In to a detailed GDPR Compliance Action Plan	• Identify appropriate senior level representatives of relevant organizations to participate – IT, Legal, HR, Finance, Marketing, etc. • Develop and adopt a Compliance Action Plan and timeline enabling identification and implementation of appropriate operational modifications prior to May 2018
Conduct a Personal Data Inventory and Review	• Identify all Personal Data collected, maintained or in the possession of the company or its vendors • Determine whether the entity is a Data Controller or a Data Processor, or both, with respect to the relevant information • Identify and document the lawful basis for processing of the Personal Data identified – if no lawful basis, the information should be deleted • Identify the databases where Personal Data is stored • Identify the personnel with responsibility for maintenance of the relevant databases • Identify data retention policies and practices • Determine level of protections built into the relevant databases • Develop list of required changes based upon the Inventory and Review. • Develop implementation plan and responsibility for required changes or modify business practices to remove the non-compliant activity
Review and Update Privacy Policy and other public statements of privacy practices	• Identify all internal and public facing documentation addressing the privacy and data protection practices of the company • Make any appropriate changes necessary for GDPR compliance

Required/Recommended Action	Activity Involved/Comments
Consent Process Review	· Review all previously obtained consents to determine adequacy under the GDPR consent requirements. · Consent must be obtained for each category or type of processing to be undertaken. · Established or existing business relationship "implied consent" no longer available · Generally, any previously obtained consent will be inadequate · See Attachment 3
New Consent Process	· Develop and implement GDPR compliant consent procedures for all processing contemplated by the business · Ability to process Personal Data post-May 2018 depends on completion of these consent procedures · Includes, email campaigns and any other use or sharing of Personal Data · Includes ability for Data Subjects to "change their mind" and revoke or condition or limit any consent previously provided
Vendor Contract Review	· Review all existing contractual arrangements with any third party that processes Personal Data on company's behalf or on whose behalf the company processes Personal Data · Determine whether the company is a Data Controller, a Data Processor or both · Modify or amend existing contracts to include required and appropriate data security provisions. · Review and modify all contract templates to ensure inclusion of appropriate data protection and information security provisions for future contracts
Data Subject Inspection Right Process	· Develop and implement a process pursuant to which Data Subjects are able to review the Personal Data processed by the company and its vendors · Develop and implement a process for assessing and responding to Data Subject requests for modification or deletion of Personal Data
Trans-border Data Transfers	· Identify all instances of transfer of Personal Data outside of the EU · Analyze all such instances for compliance with GDPR requirements · Modify or terminate any such transfers that do not comply with GDPR requirements

Required/Recommended Action	Activity Involved/Comments
	• Appropriate GDPR-compliant protections include – an adequacy determination (Privacy Shield or the like); inclusion of prescribed "standard contractual clauses;" or binding corporate rules adopted by sender and the recipient.
Data Security Breaches	• Develop a Data Security Breach Action Plan designed and effective to identify any actual or potential unauthorized or unlawful processing of Personal Data • The Plan must include a process for notifying the potentially impacted Data Subjects and relevant law enforcement or governmental officials, when required • The Plan must include a process for the conduct of an appropriate investigation and the taking of appropriate remedial actions • While applicable in the GDPR, this requirement has counterparts in most of the states in the United States – requirements which must also be contemplated and addressed in the Plan.
General Operations Review – Post Implementation	• Review all facets of the operations of the business to confirm operational consistency with modified privacy and data protection policies and procedures • Make any necessary changes to operational practices to align with GDPR-compliant policies and procedures

ATTACHMENT 3

CONSENT REQUIREMENTS UNDER THE GDPR

All processing of Personal Data requires either the consent of the Data Subject or another lawful basis for processing. Consent means any freely given, specific and unambiguous informed consent to the specified processing of specified Personal Data for specified purposes. Consent cannot be implied and requires a clear affirmative action by the Data Subject. "Freely given" means that the Data Subject must have a meaningful choice. For example, a wide-ranging consent as a condition of employment or receipt of governmental benefits will not be viewed as freely given. In order for the consent to be deemed freely given, the consent must apply only to Personal Data that is actually required for the receipt of the service or benefit to be received.

The consent should, at a minimum, identify the Data Controller and ideally, the names of or descriptions of any Data Processor. The nature of the processing should be explained in clear and plain language. Silence, pre-checked boxes, inactivity or passive acquiescence will not be viewed as valid consent. The request for consent must be obvious and cannot be "buried in the fine print."

Data Subjects must be given the right to withdraw or modify consent, which right must be included in the communication requesting consent.

While the validity of a consent will be dependent on the facts and circumstances of the particular situation, the following format for a consent can be valid if properly drafted and implemented.

[NAME OF DATA CONTROLLER] requests your consent to the collection and use of [DESCRIBE THE SPECIFIC PERSONAL DATA TO BE COLLECTED – "THE INFORMATION PROVIDED IN DURING REGISTRATION"] to [INSERT SPECIFIC USES TO BE MADE OF THE DATA – FOR EXAMPLE, "TO CONTACT YOU FOLLOWING THE EVENT TO DISCUSS POTENTIAL BUSINESS ACTIVITIES"].

This information will be made available to [IDENTIFY SPECIFIC OR GENERIC RECIPIENTS, "EXHIBITORS WHOSE BOOTHS YOU VISIT AT THE EVENT"] for these purposes. We have contracted with third parties to assist in the collection and use of your Personal Data and our contracts with these third parties require that they protect and use your Personal Data only as described in this consent.

You can refuse to provide your consent to the use of your Personal Data as described above or you can change your mind and notify us of that decision. You are reminded that if you do not provide your consent or if you change your mind, your ability to enjoy the benefits of [THE EVENT] will likely be reduced.

By checking the consent box below, you will have given your express, affirmative, freely given consent to the use of your Personal Data as described above.

ATTACHMENT 4

FINES FOR FAILURE TO COMPLY WITH THE GDPR

Article 83 of the GDPR provides details of the potential administrative fines. There are two tiers as follows – (1) up to €10 million or 2% of annual global turnover of the previous year, whichever is higher; and (2) up to €20 million or 4% of annual global turnover of the previous year, whichever is higher. While not beyond doubt, it is generally anticipated that breaches of DC or DP obligations will be fined within the first tier, and breaches of Data Subjects' rights and freedoms (e.g., malicious or intentional use of Personal Data for purposes not included in a consent or use of Personal Data without consent) will result in the higher level fine. It is important to note that these figures are the maximum figures and that there are a range of enforcement actions available short of fines. These include:

- Issuance of warnings;
- Issuance of reprimands; and
- Order compliance with Data Subject requests.

It is possible that early cases of non-compliance will result in significant fines to set a precedent, although the ability to demonstrate good faith efforts to comply with the requirements of the GDPR will also likely be taken into account. Of course, a number of criteria will be considered when determining any fine, including the nature, gravity, duration and character of the infringement. Supervising authorities may also take into account the types of Personal Data involved, any previous infringements and level of co-operation.
The amount of the fine to be imposed will be determined on a case by case basis, but the behavior and co-operation of the organization will likely be taken into account when determining the value of the fine.