TASC GDPR Privacy Policy Statement

General Data Protection Regulation (GDPR)

The new EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and will impact every organisation which holds or processes personal data. It will introduce new responsibilities, including the need to demonstrate compliance, more stringent enforcement and substantially increased penalties than the current Data Protection Acts (DPA) which it will supersede.

TASC places a high priority on protecting and managing data, especially that of its clients and employees.

TASC is focusing on the following GDPR requirements.

- Ensuring Privacy by design is implemented in all new research projects.
- Fine tuning processes to ensure they meet GDPR requirements.
- Updating our third party contract terms and conditions to reflect GDPR requirements
- Updating our Privacy Standard Policy and Privacy Notices.
- Ensuring the required consent and preferences have been requested where necessary.
- Providing guidance on data retention periods.
- Providing training for all staff to enable them to understand the requirements of GDPR and how to manage the data that they are responsible for effectively.

We are also working on an Information Security framework which combines controls from NIST (National Institute of Standards and Technology) cybersecurity framework, ISF (Information Security Forum) and ISO2700 to ensure that data:

- is protected as it comes into TASC.
- is held securely whilst with TASC.
- access is controlled whilst stored in our systems.
- is secured when it is sent to a third party where required.
- finally, that the data is securely destroyed once it is no longer required.

Should you have any further questions regarding this GDPR statement then please contact us using the following email address contact@tasc.ie

The Seven Principles we aim to adhere by

Echoing the current data protection regime, the GDPR relies on seven 'principles' contained in

Article 5, which will regulate the processing of personal data. In summary, these are:

1. Lawful, Fair and Transparent Processing: processing personal data needs to be based on one or several Lawful Processing Conditions (see below). The Data Subject should have full and transparent knowledge of the identity of the parties to the processing, the purposes of the processing, the recipients of personal data, the existence of Data Subject rights and freedoms, and how to contact the Controller. For example, a Data Controller cannot collect an email address for a newsletter subscription without giving full information on the type of processing which will occur.

2. Specified and Lawful Purpose: personal data must be processed only on the basis of one or several specified purposes. For example, data which is collected for the purpose of a newsletter cannot automatically be used to target the Data Subject with regular fundraising campaigns.

3. Minimisation of Processing: processing of personal data should be adequate, relevant and restricted to what is necessary in relation to the purposes for which they are processed. Not only will this relieve the organisation of the burden of performing actions on personal data, which are not required or necessary, but it will also reduce the overall risk of data breaches. For example, where a non-profit organisation wishes to ensure that the Data Subject is not a child, it may not be necessary to collect the date of birth of the Data Subject. A year of birth can be provided or the Data Subject can simply confirm at registration that he or she is over the legitimate age.

4. Accuracy: personal data shall be accurate and where necessary kept up to date. Non-profits should rectify any incorrect data and erase any data, which is known to be erroneous or obsolete. This will result in the Data Controller having greater confidence in the quality of data analysis, reporting and marketing campaigns.

5. Storage Limitation: personal data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. Anonymisation or deletion is encouraged in order to minimise the length of time that personal data is held by the organisation. Some identifiable data may be kept for statistical, scientific or historical research purposes. It may also be in the public interest to keep such data.

6. Security and Confidentiality: appropriate technical and organisational measures will be implemented to ensure a level of security appropriate to the volume and format of the data, its sensitivity, and the risks associated with it. For example, organisations should consider appropriate measures to protect or encrypt data when it is being taken out of the office, or transported between locations for off-site meetings. Technical measures might include password protection on files, encryption of files, CCTV security at their office, etc. Organisational measures might include limiting the amount of data that can be accessed by different teams or departments, so that data is only accessed by those who 'need to know'. Non-profits are encouraged to carry out internal security

audits and establish the risks of accidental or unlawful destruction, loss, alteration or disclosure of personal data. This includes transmissions to third parties.

7. Liability and Accountability: The Data Controller and the Data Processor will be required to demonstrate their compliance with the GDPR. As with the current legislation, the GDPR requires the Data Controller to continue to exercise reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR.

Under Article 6 of the GDPR, the processing of personal data (e.g. name, address, mobile number, e-mail address, etc.) will be considered lawful only if at least one of the following conditions applies:

- Consent: the Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes.
- Contract: the processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.
- Legal Obligation: the processing is necessary for compliance with a legal obligation to which the Controller is subject
- Vital Interests: the processing of the personal data is necessary in order to protect the vital interests of the Data Subject.
- Public Interest / Official Authority: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller (e.g. where the non-profit is acting as an agent for the Department of Social Protection, or the HSE, in providing a service).
- Legitimate Interest: the processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

Lawful Processing Conditions – Special Categories of Processing

Special categories of processing (processing of medical information, or information relating to race, religion, political beliefs, etc.), receive an additional level of protection under the GDPR.

Such processing must be justifiable with reference to at least one condition from Article 9 of the Regulation – if this cannot be done, then the organisation should not be processing such information.

For example, when processing these special categories of personal data, the consent of the Data Subject needs to be explicit and cannot be implied or assumed.

The full list of Conditions from Article 9 is as follows:

1. The Data Subject has given explicit consent to the processing of those personal data for one or more specified purposes; or
2. The processing is necessary for the purposes of carrying out the obligations of the Controller or of the Data Subject in the field of employment and social security and social protection; or
3. The processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent; or
4. The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim, in connection with its ethos and purposes; or
5. The processing relates to personal data which are manifestly made public by the Data

Subject; or

1. The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or
2. The processing is necessary for reasons of substantial public interest; or
3. The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services pursuant to contract with a health professional; or
4. The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or
5. The processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with the Regulation.

Consent - Current Law

In preparation for the GDPR, organisations are advised to check the quality of the personal data they hold, and the quality of consent for direct marketing purposes in particular. One of the primary sources of complaints with the Office of the Irish Data Protection Commissioner is the lack of clear consent for electronic direct marketing, i.e. the recipient of a promotional message disputing the fact that they ever gave consent, or claiming that they had declined to give consent and were nonetheless contacted.

Aside from using data for Direct Marketing purposes, many non-profits rely on the consent of their service users on a day-to-day basis. It is important, therefore, that this consent is freely given and that the implications of giving consent are clearly understood by the Data Subject.

In the context of Direct Marketing, the current legislation differentiates between new and existing customers or donors when it comes to consent:

New Customers or Donors	Existing Customers or Donors
Post: No prior consent required, but all promotional messages must offer the recipient a free and easy-to-use option to opt out from receiving further messages.	**Post:** No prior consent is required, as long as the individual was given the option to opt out at the time their data was acquired. All promotional messages must offer the recipient a free and easy-to-use option to opt out from receiving further messages.
SMS messages and e-mail: Explicit prior consent is required to use personal contact details for marketing purposes; where consent is received, use the data for that purpose at least once in each 12-month period; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.	**SMS messages and e-mail:** Explicit prior consent is required. Where such consent was given, recipient must have had the option to opt out at the time their data was acquired initially, as well as in subsequent marketing messages. Personal data can continue to be used for direct marketing purposes if the data is used for that purpose at least once in each 12-month period from the date it is acquired; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.
Calls to land-line and mobile phones: Prior and explicit consent is required for marketing where the number is listed in the National Directory Database (NDD). Where consent is given, data for that purpose must be used at least once in each 12-month period; and each time the recipient must get a free and easy-to-use option to opt out from receiving further messages. No prior consent is needed where the number is not on the NDD.	**Calls to land-line and mobile phones:** Where such consent was given at acquisition, recipient must have had the option to opt out at the time their data was acquired initially, as well as in subsequent marketing messages. Personal data can continue to be used for direct marketing purposes if the data is used for that purpose at least once in each 12-month period from the date it is acquired; and each message must remind the recipient that they have a free and easy-to-use option to opt out from receiving further messages.

When it comes to direct marketing, the 'double opt-in' principle applies to all Irish non-profit organisations. It is not sufficient that an individual donates to a particular organisation or campaign in order for their details to be added to your direct marketing list – **separate, clear consent must be acquired for this purpose.**

Consent under the GDPR

The GDPR, which came into force in May 2018, introduces a new definition of consent for all purposes, not just Direct Marketing.

Consent will now be any 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4.11).

In order to comply with this standard, organisations will need to be able to:

- Explain when and how they acquired the personal data of the Data Subject;
- Explain the purpose or purposes for which the data was acquired;
- Demonstrate the quality of the consent they have received (this requires organisations to keep a record of the interaction with the Data Subject at the point of collecting his or her consent).

These more stringent criteria are likely to raise some challenges for organisations with regard to the consent they have for marketing and other purposes. There is a natural concern that the data they currently hold will not meet these stricter criteria. The guidance from the Office of the Irish Data Protection Commissioner is that data can only continue to be used for Direct Marketing purposes where the quality of consent can be shown to meet this standard. In this regard, the GDPR states in a recital that processing, which is already under way on 25 May 2018, should be brought into conformity with the Regulation.

This will mean that organisations will need to review the quality of the data they already hold, and ensure that it meets the new consent criteria prior to May, 2018. Otherwise, it may no longer be possible to use consent as the basis for processing the data, and another Lawful Condition will need to be provided for that purpose.

Where processing is based on consent, it is not necessary for the Data Subject to give his or her consent again if the original consent is in line with the conditions of the Regulation. In such circumstances, the Controller can simply continue to use the data as before.

However, where the original consent does not meet these criteria, it may be necessary to conduct a data quality review prior to May 2018, as outlined below.

Obligations on Data Controllers

Whilst some liability may be apportioned to the Data Processor or another Joint Controller, the Data Controller is the party which is principally responsible for the processing of the data in question.

Key responsibilities will include:

- Process logging: every processing activity needs to be recorded in a tracking system, which is maintained on an ongoing basis; adequate, documented reports on such processing activity needs to be available when requested by the Office of the Data Protection Commissioner (unannounced audits are permissible under the GDPR); the log must include such details as the parties involved, the purpose of the processing, the categories of personal data and Data Subjects, the recipients, any transfers outside the European Union, and so forth. As such, the

obligation to document a data processing log replaces the current system of registering with the Office of the Data Protection

- Commissioner. The Processing log becomes a key mechanism to demonstrate compliance in the future. Process Logging only applies to organisations with more than 250 employees, but some smaller organisations, including non-profit organisations, will also have this obligation where they regularly process sensitive data or conduct special categories of processing.
- Logging breaches: any personal data breaches of which the Controller or Processor are aware must be documented, in line with the processing log system described above.
- Breach notification to the Office of the Data Protection Commissioner: only breaches which are likely 'to result in a risk for the rights and freedoms of individuals' will need to be reported, but that is a broad definition and the deadline is 72 hours from becoming aware of such an incident. Any delay in reporting, beyond that point, must be explained with a reasonable justification.
- Breach notification to the Data Subject: such notification, which must be given 'without undue delay', must be made where the Controller is aware of an incident which exposes the data or the rights and freedoms of the Data Subject to risk. Certain encryption or pseudonymisation techniques may prevent the Controller or Processor from having to notify the Data Subject, e.g. where a device containing personal data is lost or stolen, but the device itself is encrypted, the data is considered safe and no notification to the Data Subjects is necessary.
- Data Processing Contracts: the GDPR will require the Controller to enter into a Data Processing Agreement with each Data Processor who is involved in the processing of personal data on the Controller's behalf. This contract needs to be in writing and must cover certain basic requirements, such as guarantees concerning the safety and security of data, auditing rights, cooperation concerning the rights and freedoms of Data Subjects and so forth. A similar written agreement needs to be put in place where the Controller enters other arrangements, e.g. between two non-profits in a group hierarchy; between Joint Controllers or where several Processors work together in one processing activity.
- Sub-contracting: the Controller needs to be aware that where a Data Processor enlists another processor for carrying out specific processing activities on behalf of the Controller, it will be the responsibility for that Processor to ensure that the same level of protection exists for the data during this element of the processing, as exists between the Controller and the initial Processor. In the community, voluntary and charity sector, an example could be where a data analytics company carries out a profiling activity on a database belonging to a non-profit, but in turn uses a self-employed consultant who works side-by-side with its in-house employees. In this case, the clauses of the data processing agreement between non-profit and the analytics company must be mirrored in the data processing agreement between the analytics company and the self-employed consultant.
- Privacy Impact Assessments: where a significant change to data processing operations are likely to result in a high risk to the rights and freedoms of the Data Subject, the Data Controller will be required to carry out a Privacy Impact Assessment in order to evaluate the risks inherent in such changes. In particular, attention has to be given to the origin, the nature and the severity of the risk in question.
- The results of this Impact Assessment must be documented and retained, and must be made available to the Office of the DP Commissioner (ODPC) on request. Any identified 'high risk' has

to result in the Controller engaging with the ODPC before the processing activity in question begins.

- Data Protection by Design and Default: in line with the requirement to carry out a Privacy Impact Assessment, the principles of 'Data Protection by Design' and 'Data Protection by Default' place privacy and the rights and freedoms of the Data Subject at the heart of any current or future processing activity. In a non-profit context, this can include direct marketing, fundraising, profiling, analytics, outsourcing of services and upgrading of the back office database. It may also capture all data processing activities and how, after writing processing logs, the organisation intends to minimise any processing in question and ensure that no unnecessary actions on personal data are taken.

Our Do's and Don'ts for TASC

DO!	DON'T!
Do carry out an assessment and prepare for the GDPR in a systematic manner on the basis of identified risks. This legislation introduces a wide range of changes to data protection compliance.	Don't leave it to the last minute - your organisation handles more data and in more complex ways than you might think, and it will take time to get ready for the GDPR!
Do appoint a Data Protection Officer or 'Champion' as soon as possible to take ownership of this compliance project.	Don't allow an untidy database to drag down your compliance standards and your good reputation.
Do check your lawful processing conditions, the quality of your consents and recording these consents on your database.	Don't forget to invest in staff training: according to studies, human error accounts for more breaches than cyberattacks or technical malfunctions combined.
Do include all aspects of your organisation in your compliance, as data protection reaches from reception all the way to management.	Don't transfer data to a country outside the EU without adequate safeguards.
Do carry out Privacy Impact Assessments and build 'privacy by design' into all your projects.	Don't process data with others without having an appropriate data processing agreement in place.
Do log your data processing activities in a tailored process logging system or report.	Don't miss the opportunity, where possible, to apportion some element of liability to other entities.
Do prepare for Subject Access Requests, the Right to be Forgotten, the Right to Opt out of Profiling and other Data Subject rights and freedoms.	Don't merge servicing and direct marketing communication into one undefined message.
Do put in place systematic data breach prevention systems and data breach notification systems. Consider both physical measures (locks and CCTV), organisational measures (different authorisation levels for staff) and technological solutions (password protection, back-ups and encryption)	Don't put your head in the sand when a breach occurs - transparently communicate with the Office of the Data Protection Commissioner and the Data Subject, where necessary, to prevent further escalation or recurrence.
Do take part in the wider national debate on data protection in the Irish community, voluntary and charity sector – network with others in your sector, attend conferences, breakfast briefings and other events which can help you stay up to date.	Don't disregard the sanctions and fines of the GDPR, as they can be significant and will apply equally to the nonprofit and 'for profit' sectors.

Approved at Board Meeting Date: 18.09.20
Signed by Chair: Mike Jennings
Signature: