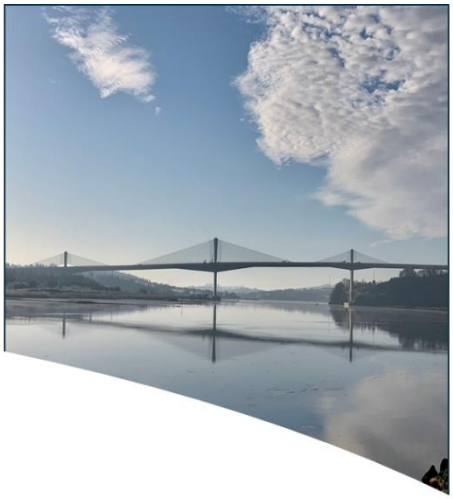
Policy Document

Data Policy and GDPR Compliance



McCURDY associates

April 2021

Table of Contents

List of Tables

Appendices

1 Introduction

1.1 General

The production of this document has been prompted by the introduction of the General Data Protection Regulations (GDPR) which came into force on 25th May 2018. This document is intended to set out how we are compliant with the GDPR.

In essence, we do not collect, process or use private data on the scale or to extent that this Regulation is specifically interested in. That is, our business is not in the processing of private data for commercial gain. Our business is focussed on providing expert technical advice for which the processing of private data is essentially constrained to maintaining communications with colleagues, clients and partners or subcontractors.

Nevertheless, as a European organisation, McCurdy Associates Consulting Engineers Ltd. ("MACEL") is bound by this Regulation and must therefore do what it can to ensure its compliance.

The process of achieving compliance has resulted in useful consideration of the way in which data is used, stored and protected, and this will add further to the resilience and robustness of the business. Therefore, the risks, mitigations and activities identified here must be maintained, improved and reviewed regularly to ensure that we not only protect MACEL, but also its clients and colleagues from personal data falling into the wrong hands.

It is therefore critical that all employees and associates of MACEL are aware of their obligations under this document and comply with it.

1.2 Context

The General Data Protection Regulations (GDPR)[1] came into force on 25th May 2018. Failure to comply with these regulations from that date carries the potential for serious fines of up to €20m or 4% of global turnover, whichever is the greater. It is therefore essential that MACEL can comply with these regulations and to be working within its obligations from that date.

1.3 Methodology

This document has been developed with reference to the Regulation and using guidance provided by the Data Protection Commission (DPC)[2] as identified within the text by footnotes or hyperlinks. It has not been reasonably practicable to read all the documentation produced by these two organisations, but we have identified and selected documents that appear to be most relevant and incorporated that guidance into this document.

This document will be reviewed and updated should any changes be made to legislation.

1.4 Purpose and structure of this document

The purpose of this document is to set out the actions that must be taken to be compliant with the GDPR's obligations.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en
[2]https://www.dataprotection.ie/#:~:text=The%20Data%20Protection%20Commission&text=The%20DPC%20is%20the%20Irish,as%20the%20Law%20Enforcement%20Directive.

2 Data Policy

2.1 General

This Policy is intended to comply with the GDPR requirements and uphold the rights of individuals contained within it. It has been developed in good faith but without formal legal advice.

The basic data management principles we abide by are:

- We will only collect and retain such personal data as is necessary for the performance of our work and operation of the business.
- We will only give access to those that need it for the performance of their work.
- We will take reasonable steps to ensure the security of that data is not compromised in use, storage, or transit.
- We will report actual or suspected data security breaches to the DPC within 72 hours or 24 hours if practicable.
- We will uphold the rights of individuals under the GDPR.

3 Formal Roles

3.1 Controller

The Controller for MACEL is Áine Walsh as Director of MACEL.

3.2 Processor

MACEL does not engage in bulk or external processing of private data and therefore does not have a formal Processor. Processing is generally restricted to the entry, correction or deletion of contact details on an individual record basis.

3.3 Data Protection Officer (DPO)

DPC guidance states that you must designate a DPO in certain circumstances. Since MACEL does not fit any of these conditions, a DPO is not necessary.

4 Privacy Notices

4.1 General

The following contains the text to be extracted and used in various Privacy Notices used for Staff, Clients, and Subcontractors. These are followed by more general notices for the company website and email footers. This information has been derived from the Schedule of Processing, Personal Data and Data Subjects audit contained in Appendix A.

4.2 How privacy notices will be made available

For staff, the privacy notice is included in the HR policies.

For Clients, the privacy notice will be included in tender proposals.

For any subcontractors, the privacy notice will be provided when a subcontractor is formally invited to work for MACEL.

For website users, the text will be contained in the standard footer of each page and the 'Contact Us' page.

For email contacts, the text will be contained in the standard 'New' and 'Reply' email footers.

4.3 Staff privacy notice

4.3.1 What information do we hold about you and why do we hold it?

The personal information we hold about you is limited to:

Table 4-1: Staff private information

Information we hold	Why we hold it
Name	We need to be able to identify you legally
Gender	Some clients require company gender statistics as part of their prequalification process.
Personal address	For personal communication e.g. pay
Personal mobile number	For personal communication before and after employment or contact if company contact information is not working
Personal email address	For personal communication before and after employment or contact if company contact information is not working
Next of kin contact details	For contact in emergency situations only e.g. if you suffer from serious illness or death while under company protection
PPS No.	For compliance with Irish tax requirements
Bank account details	To pay you
Copy of passport	To demonstrate your right to work in the Republic of Ireland and arrangement of any visas for foreign travel
Photo	Needed for marketing purposes (e.g. Website, LinkedIn, CVs)
CV	Needed for issue to potential clients as part of project tenders or contracts

4.3.2 How do we use your personal information?

For the avoidance of doubt, we do not automatically process your information, nor do we analyse it or sell it to other parties.

We may make your name, CV and photo available to clients or organisations we are collaborating with but only for the purposes of winning or delivering work. All other information will not be made available to any other party without your direct permission unless required by law.

At the end of your employment with us, we will only hold onto information that is directly needed to fulfil our legal tax, reporting or audit obligations and to complete any outstanding payments.

4.3.3 On what legal basis do we hold your information?

The legal basis we hold this information is 'Legitimate interests' on the grounds that we need this to be able to pay you, deliver work for clients, and win work.

4.3.4 What are your rights?

Your rights are as contained in the European Data Protection Regulations and include your rights to freely access information about you within reasonable timeframes.

4.4 Client privacy notice

4.4.1 What information do we hold about you and why do we hold it?

The personal information we hold about you is limited to that listed in Table 4-2:

Table 4-2: Client private information

Information we hold	Why we hold it
Name	We need to be able to communicate with you
Company contact details (Job title, address, mobile/landline numbers, email addresses)	For business-related communications
Personal mobile number	We will only hold this if you have personally provided it to us and advised us to make use of it if necessary

4.4.2 How do we use your personal information?

For the avoidance of doubt, we do not automatically process your information, nor do we analyse it or sell it to other parties.

This information will not be made available to any other party without your direct permission unless required by law.

We will retain information that is directly needed to fulfil our legal tax, reporting or audit obligations. We may use your contact details to provide marketing information to you about our services and capabilities from time to time.

For more information about how we maintain the security of your information, please contact Áine Walsh.

4.4.3 On what legal basis do we hold your information?

The legal basis we hold this information is ‘Legitimate interests’ on the grounds that we need this to be able to provide our services and maintain business communications with you.

4.4.4 What are your rights?

Your rights are as contained in the European Data Protection Regulations and include your rights to freely access information about you within reasonable timeframes for accessibility.

If you do not wish to receive marketing information from us, please advise us and we will remove your name from our marketing list.

4.5 Associates and other sub-contractors privacy notice

4.5.1 What information do we hold about you and why do we hold it?

The personal information we hold about you is limited to that shown in Table 4-3:

Table 4-3: Associate and sub-contractor private information

Information we hold	Why we hold it
Name	We need to be able to communicate with you
Company contact details (Job title, address, mobile/landline numbers, email addresses)	For business-related communications
Personal mobile number	We will only hold this if you have personally provided it to us and advised us to make use of it if necessary
Company bank account details	To pay you
Copy of passport (if requested)	To demonstrate your right to work in the Republic of Ireland and arrangement of any visas for foreign travel
CV	Needed for issue to potential clients as part of project tenders or contracts
Copies of company insurance certificates*	To assure ourselves and our clients that you have sufficient insurance cover to meet the terms of the contract
Company registration number*	To be able to confirm that the business is a legitimate business and a going concern. This information is often required on Government prequalification forms for all subcontractors as well as direct contractors.
Company VAT number*	This information is often required on Government prequalification forms for all subcontractors as well as direct contractors.
Company bank account details*	We need this to pay you

* this information is not visible to other Associate or subcontractors and is visible only to your organisation lead and MACEL management and any nominated project administrators who need access to it for administrative purposes, including paying the associate or subcontractors[3].

4.5.2 How do we use your personal information?

For the avoidance of doubt, we do not automatically process your information or sell it to other parties. We may use it to check credit ratings and confirm that your company is (or remains to be) a legitimate organisation and a going concern.

We may make your name, CV and photo available to clients or organisations we are collaborating with but only for the purposes of winning or delivering work. All other information will not be made available to any other party without your direct permission unless required by law.

At the end of your contract with us, we will only hold onto information that is directly needed to fulfil our legal tax, reporting or audit obligations and to complete any outstanding payments.

For more information about how we maintain the security of your information, please contact Áine Walsh.

4.5.3 On what legal basis do we hold your information?

The legal basis we hold this information is ‘Legitimate interests’ on the grounds that we need this to be able to pay you, deliver work for clients, and win work.

[3] This is currently Samuel McCurdy and Áine Walsh.

4.5.4 What are your rights?

Your rights are as contained in the European Data Protection Regulations and include your rights to freely access information about you within reasonable timeframes for accessibility.

4.6 Website users

4.6.1 All web page footers

This website does not collect Cookies, but we do use Google Analytics to understand how visitors use the site. None of this can be traced to any individual user. or more detail on our Privacy Statement please visit the 'Contact us' page.

4.6.2 Contact us page

Privacy Statement

We are committed to protecting your privacy. Before providing us with any of your details, please read the following important information which concerns the protection of your personal data.

We will hold and process any personal information which you provide via the site or by submitting emails and/or online forms for our own internal business purposes. We do not pass on or sell online personal information to third parties. We may however share information within our organisation. This may include our employees, agents, contractors and sub-contractors. Please note that by sending your personal information to us you are explicitly consenting to the processing and transfer of such information in this way.

In addition to the information you submit to us via the site, we may collect information about visits to the site. We collect information on the page browser access and gather information on the relative popularity of each page, the average number of pages accessed by visitors, the average time spent on the site and similar information related to the way in which the website is used. None of this information is linked back to you as an individual.

We may provide hyperlinks from the site to websites of third parties. Please note that this privacy statement applies only to the contents of the site and not to those web sites to which we may provide a link.

We are willing, on written request from you, to provide details of any personal information which you have provided us with and/or to cease to make use of your personal information for the purposes described above. We may require proof of identity from you prior to disclosing such information. This is to safeguard the security of your information. You should send any request to aine.walsh@mccurdy.ie.

If any information with which you have provided us becomes inaccurate or out of date, or if you have any queries about this privacy statement, please contact us via this website or the contact details provided on this page.

4.6.3 Email footer notice

Email Disclaimer: The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and maybe unlawful. If you received this in error, please contact the sender and delete the material from any computer. When addressed to our clients any opinions or advice contained in this email are subject to the terms and conditions expressed in the governing Agreement. McCurdy Associates are neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt.

5 Individuals rights and access

5.1 General

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

If an individual wishes to review the information we hold for them, it will be provided free of charge within the appropriate timescales but generally within one working day should be practicable.

Since we do no major processing of private information, amendments should be as simple as identifying the contact in the address book and making the changes, including deletion.

Other records including email communications, minutes, reports etc. may be retained for legal audit purposes for at least 6 years.

6 Data Breaches

6.1 Where is private data held?

Private information data is principally held on computer and a mobile phone, backed up via the cloud. Private data locations are shown in Table 6-1.

Table 6-1: Private data locations

Software	Information
Dropbox	CV's, calculations, current projects, archived projects, quality documents, management documents, business development, company records
MS Office Outlook	Contact details, email records, diary
Sage One	Accounting information including invoices
MS teams	Contact details, chat records, diary
Harvest	Timesheets, expenses

6.2 What security measures are in place?

Security measures in place are shown in Table 6-2.

Table 6-2: Security measures in place

Security measures	Purpose
MACEL staff/ associates/ sub consultants only have access to the data relevant to them	To preserve confidentiality of project information and avoid Conflicts of Interest

Security measures	Purpose
Laptops are password protected (PIN number; password); Mobile is protected by password login	Prevent any user logging in
Norton Antivirus	Protects against viruses and hacking / phishing
Automatic updates of Windows / Microsoft and other software	Prevent security flaws in software being exploited
Tag & Track stickers on all IT and valuable equipment; Company contact details on laptops.	Enable lost property to be identified and returned
Office is locked. Access is by fob. Laptops are not left in office overnight.	Prevent unauthorised access without significant damage
Staff only have access to directories they need to for their work	Avoid unnecessary exposure of risk or potential for false accusation

6.3 What are the data security risks and mitigations?

Data security risk assessment is shown in Table 6-3.

Table 6-3: Data security risk assessment

Event	Outcome	Pre-mitigation risk	Mitigations	Post-mitigation risk
Laptop is lost or stolen and used by experts with malicious intent	Access to data is gained	Low	Password protect laptop.	Very Low
Mobile is lost stolen and used by experts with malicious intent	Access to data is gained	Low	Enable remote locate and wipe technology and maintain separate recovery process info in the cloud	Very low
Office is broken into	Access to equipment and hard copy records.	Low	Retain hard copy details and minimise number of hard copies. Bring laptops home each evening.	Very low
Member of staff makes private information available to others by accident or malicious intent	Confidential data is made available to those who should not have it	Very Low	Staff only have access to information they need and are made aware through the HR policies of the confidentiality and due care obligations	Very low
Laptop is hacked remotely (MACEL may not be aware)	Access to data is gained	Very low given the existing control mechanisms	Enable 2nd means of authentication for Google and MS Office software	Very low

6.4 What happens if a data breach is suspected or confirmed?

Any MACEL employee, associate or sub-consultant aware of a suspected or actual data breach must inform the Director of MACEL at the earliest possible opportunity, and in any case with enough time to inform the DPC within 72 hours as MACEL is required to do by law and MACEL will face a fine if it has not proactively contacted the DPC in this event.

Examples include:

- Leaving a laptop or phone or confidential document on a train
- Emailing the wrong person
- Sharing third party contact information without the individual's express consent

It is therefore critically important that any employee should recognise that any potential data breach must be communicated as soon as possible, together with an assessment of:

- what information is likely to be accessible;
- who it might affect; and
- the likely damage that will occur.

The Director of MACEL will then need to report this to the DPC along with a statement of the actions subsequently taken, and remaining actions to limit the potential for damage.

7 Data Protection

7.1 Data protection by design

The normal basis upon which private data is collected and used is within software that provides a built-in level of security that is reasonable for the purposes for which it is used. By restricting data access to only those that need it, we have built in data protection by design.

7.2 Data Protection Impact Assessment (DPIA)

Based on information published by the DPC, we have concluded that none of the data retained or processed is 'likely to result in a high risk to the rights and freedoms of natural persons' and therefore a Data Protection Impact Assessment (DPIA) is not necessary at this time. If, however, circumstances change either in the requirement for a DPIA or the way in which data is handled or the type of data handled, we will review this requirement again.

8 Lead data protection supervisory authority

8.1 Which organisation is the lead data protection supervisory authority?

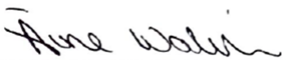
The DPC in the Republic of Ireland.

8.2 Where is MACEL's 'main establishment'?

In Kilkenny, Ireland – although a lead data protection supervisory authority is not actually necessary as we do not carry out cross-border processing between different MACEL offices.

9 Signature

Signed:



Áine Walsh
Director
McCurdy Associates Consulting Engineers Limited
10 Ormonde St.
Kilkenny
Ireland
R95 R2HY

Date: 13th April 2021

Appendix A: Schedule of Processing Personal Data and Data Subjects

Schedule of processing, personal data and data subjects

Description	Details	Staff	(Potential) Client	(Potential) associate/ sub-consultant
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter]	Personal and payment details	Contact and Contract details	Contact and Contract details, as well as payment details
Duration of the processing	[Clearly set out the duration of the processing including dates]	Dates of employment	Retained for up to 6 years from date of contract completion or payment of last invoice, whichever is the later	Retained for up to 6 years from date of contract completion or payment of last invoice, whichever is the later
Nature and purposes of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]	Collected for the purposes of compliance with employment law and processing of employment-based payments Image required for publicity and CV purposes	Collected for the purposes of fulfilment of the contract, and records in the event that a liability claim is made	Collected for the purposes of fulfilment of the contract, and records in the event that a liability claim is made
Type of personal data	[Examples here include: name, address, date of birth, PPS number, telephone number, pay, images, biometric data etc]	Name Home address Date of Birth PPS number Personal mobile and landline number Personal email address Photo Passport scan Pay CV	Name Address Email Contact telephone numbers Company position / job title Notes relating to previous contact discussions	Name Address Email Contact telephone numbers Company position / job title Notes relating to previous contact discussions
Categories of data subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients,	Staff	Client	Subcontractor

Description	Details	Staff	(Potential) Client	(Potential) associate/ sub-consultant
	students / pupils, members of the public, users of a particular website etc]			
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	[Describe how long the data will be retained for, how it be returned or destroyed]	All personal data except for photo ID to be retained for 18 months from leaving date to ensure that accounts can be completed. Any further retention of this data beyond that time will be for statutory purposes only. Photos will be deleted within one month of the employees leaving date.	Contact information data to be retained as per duration above to allow communication if there were to be a liability claim. After that, and at any time if no contract exists, all data may be deleted on request by the client	Contact information data to be retained as per duration above to allow communication if there were to be a liability claim. After that, and at any time if no contract exists, all data may be deleted on request by the subcontractor