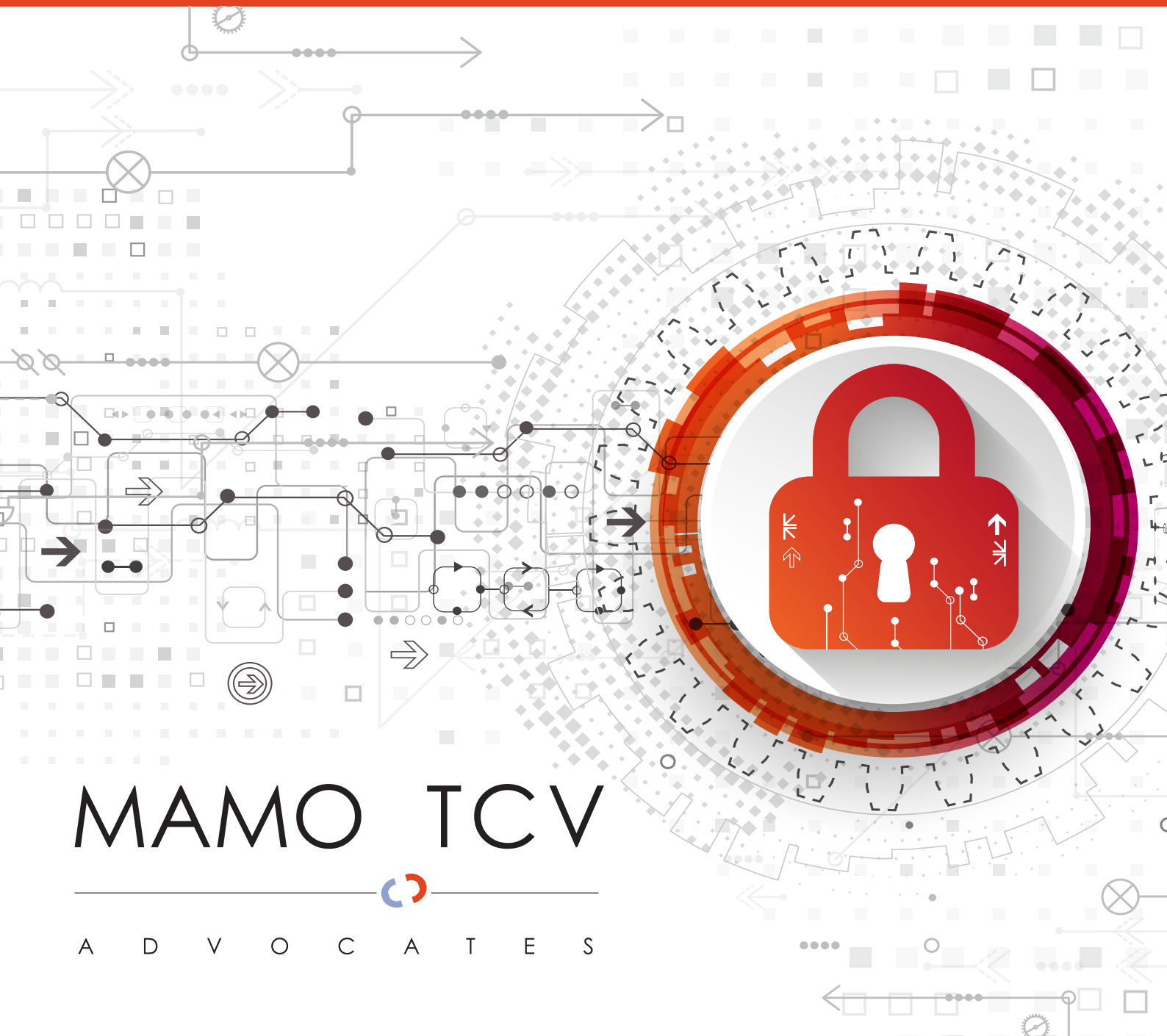
A Brief Overview of the **EU General Data Protection Regulation (GDPR)**

5th Edition

January 2021



MAMO TCV

ADVOCATES

www.gdprmalta.com

Check the link above for any updated versions of this overview.

What is the 'GDPR'?

The General Data Protection Regulation or '**GDPR**' (Regulation 2016/679/EU) is a single EU law dealing with data protection that came into effect across the EU, including Malta, on **25 May 2018**. The GDPR repealed Directive 95/46/EC and the domestic laws implementing the same. The Maltese Data Protection Act, 2018 (Chapter 586 of the Laws of Malta) has also come into effect replacing the former Data Protection Act (Chapter 440 of the Laws of Malta).

The GDPR and the implementing domestic laws regulate the manner in which the **personal data** of **data subjects** are **processed** by **data controllers** and **data processors**. The main goal of the GDPR was to *increase* the privacy rights of natural persons and to keep up with the digital age we live in.

Various new, and in some cases, **onerous legal obligations** were introduced by the GDPR. This document outlines some of the main changes that came into effect in Malta as a result of the coming into force of the GDPR.

This document does not purport to give legal advice. Should you require further information or legal assistance, please do not hesitate to contact us at **dataprotection@mamotcv.com**

"Some of the changes that the GDPR introduces will require some corporate restructuring and the introduction of new internal policies..."

Prof. Andrew Muscat
Partner, Mamo TCV
May 2017

"25 May 2018 will be a watershed moment in the history of EU and Maltese data protection legislation..."

Dr. Claude Micallef-Grimaud
Partner, Mamo TCV
April 2017

The GDPR at a Glance:

- Fines up to **€20,000,000.00** or **4%** of an entity's total worldwide annual turnover
- Significantly **expanded territorial scope**
- Mandatory **data breach notification** in certain cases
- Mandatory appointment of a **Data Protection Officer** in certain cases
- **Data processors** now also directly responsible at law
- More stringent **consent** requirements
- **Increased level of information** to be provided to data subjects
- More **stringent requirements** in controller-processor contracts
- Removal of the **general notification** requirement
- New **data subject rights**

What's New Under the GDPR?

Expanded Territorial Scope

Besides controllers and processors established *within* the European Union, the GDPR's reach has now been expanded to also capture organisations established *outside* the EU in the following two circumstances:

1. Where such organisations **offer goods or services** to data subjects in the EU;
2. Where such organisations **monitor the behaviour** of data subjects in the EU.

Consequently, several international organisations that previously escaped the scope of national data protection legislation are now subject to full compliance with the GDPR, regardless of where they are established.

EU data protection law now applies to many international organisations regardless of where they are established.

New Data Processor Obligations

Prior to the promulgation of the GDPR, data controllers were the entities that were mainly responsible for compliance with Maltese data protection law. Under the GDPR, action can be taken directly against defaulting data processors (i.e. those entities that process personal data on behalf of data controllers), meaning that liability no longer falls solely on data controllers and certain obligations are now imposed directly on data processors.

Moreover, among other obligations (subject to significant fines in case of default), data processors are obliged to:

- **Keep a record of all processing activities performed on behalf of the controller;**
- **Only appoint sub-processors with the written consent of the controller;**
- **Interact directly with the local Information and Data Protection Commissioner ('Commissioner') when necessary;**
- **Implement appropriate security measures to protect personal data;**
- **Notify the data controller of data breaches without undue delay;**
- **Adhere to a number of obligations to be included in data processing agreements entered into between the controller and the processor (such as the processor's obligation to demonstrate compliance with the GDPR).**

Maltese data processors are now directly answerable at law for data protection infringements.

Data Breach Notification

As a general rule introduced in Malta by the GDPR, **data controllers** must report a data breach to the Information and Data Protection Commissioner **within 72 hours of becoming aware of it**. By way of *exception* to the general rule above, breach notification to the Commissioner is not required where the data breach is unlikely to result in a **risk** to the rights and freedoms of natural persons.

Notification to the Commissioner must include, *inter alia*, a description of the breach, the number of affected data subjects, the categories of data affected, the name and contact of the Data Protection Officer ('DPO'), the likely consequences of the breach and the measures taken by the data controller to remedy or mitigate the breach.

No matter how big or small, **all breaches** (notifiable or otherwise) must be recorded, usually by the DPO, and reported to the Commissioner on demand.

The GDPR also introduced the obligation to notify affected data subjects (without undue delay) in the event of a data breach which is likely to result in a **high risk** to the rights and freedoms of natural persons. In this case, notification must include the name and contact of the DPO, the likely consequences of the breach and the measures taken by the controller to remedy or mitigate the breach.

"***It is not mandatory for all data breaches to be notified*** *to the Commissioner or the affected data subjects. This is why Controllers should seek legal advice on a case-by-case basis*."

Dr. Antoine Camilleri
Partner, Mamo TCV
May 2019

Such notification (to data subjects) will not be necessary when:

- **Risk of harm is remote because data is protected;**
- **Controller has taken measures to protect against the harm;**
- **Notification would require disproportionate efforts.**

Once a **data processor** becomes aware of any data breach, the data processor will have to notify the data controller of any such breach without undue delay. In this respect, the data controller's 72 hours will commence upon being notified by the data processor.

Therefore, Maltese organisations must carefully evaluate and, where needed, update their internal procedures to comply with these requirements. Upon becoming aware of a breach, a risk assessment should be carried out as a matter of urgency.

As a general rule, data controllers in Malta now have to notify the Information and Data Protection Commissioner and data subjects of certain data breaches and this, within very short timeframes.

New Consent Requirements

Consent requirements are stricter under the GDPR. For example, where consent is the legal basis being relied on for processing personal data, the GDPR states that consent must be given by a **statement** or by a **clear affirmative action** confirming that consent must be expressly given. This is further confirmed by the GDPR's preambles that state, *inter alia*, that "Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

Where consent is required, organisations must be able to demonstrate that unambiguous, freely given, specific and informed consent has in fact been provided. In the case of special categories of personal data (formerly referred to as 'sensitive personal data') consent must be *explicit* and not merely *unambiguous.*

Organisations must therefore scrutinise their records and check that any consent previously obtained under the former legal regime is compliant with the requirements under the GDPR. If not, fresh consent must be obtained.

The data subject must be informed of his/her right to withdraw his/her consent (at will) from the processing of his/her data at any time. In fact, under the GDPR, *"it shall be as easy to withdraw as to give consent".*

Consent requirements under the GDPR have been increased significantly. Consent must be given by a statement or a clear affirmative action. Pre-ticked boxes or inactivity do not constitute valid consent.

Data Protection Officers

Unlike the situation under the previous legal regime, the GDPR, in certain cases, mandates the appointment of a data protection officer ('DPO'), whose responsibilities include ensuring compliance with data protection law.

In terms of the GDPR, a DPO *must be appointed* if:

- **The relevant data processing operation is carried out by a public authority or body;**
- **The core activities of the controller or processor require regular and systematic monitoring of data subjects, on a large scale; or**
- **The core activities of the controller or processor involve processing of sensitive personal data or data relating to criminal convictions and offences, on a large scale.**

The appointed DPO must be suitably qualified and have sufficient authority within an organisation to carry out his/her functions. Conflicts of interest should always be avoided.

Failure to appoint a DPO when required to do so may expose an organisation to fines up to 10 million Euro or 2% of its total worldwide annual turnover.

The relevant details of the appointed DPO must be notified to the Maltese Information and Data Protection Commissioner ('IDPC').

The GDPR mandates the appointment of a DPO in certain cases and failure to do so may lead to significant fines.

Information to Data Subjects

Under the GDPR, the information provided to data subjects must be **concise, transparent, intelligible** and **easily accessible** using **clear** and **plain language**.

Where the personal data relating to the data subject are being collected *from the data subject him/herself*, the controller must provide the said data subject with, *among other things*, the following information (unless the data subject already has it):

- The **identity** and **contact details** of the **controller**;
- The **contact details** of the **data protection officer**, where applicable;
- The **purpose of the processing** for which the personal data are intended, including any 'further processing';
- The controller's **legitimate interests** (if processing is based on this legal ground);
- The **legal basis** for the processing;
- The **recipients or categories of recipients** of the personal data, if any;
- The intention to effect certain **data transfers to third countries**;
- The **data retention period** (or criteria used to determine this);
- The existence of **automated processing**, including profiling, and related information;
- The existence of **certain data subject rights** including:
  - the right of **access**;
  - the right to **rectification;**
  - the right to **erasure** ('right to be forgotten');
  - the right to **restriction of processing**;
  - the right to **data portability**;
  - the right to **object** to certain processing;
  - the right to **lodge a complaint** with a supervisory authority; and
  - the right to **withdraw consent at any time** (where processing is based on consent).
- Whether the provision of personal data is a **statutory or contractual requirement**, or a requirement **necessary** to enter into a contract; and
- Whether the data subject is **obliged** to provide the personal data and of the possible **consequences of failure to provide such data**.

Where the personal data have not been obtained from the data subject him/herself, additional provisions (including legal exceptions) apply. For example, in such cases the controller also has the obligation to inform the data subject of the **categories of personal data** concerned as well as the **source** of such personal data.

Controllers must ensure that all privacy policies, data protection notices and other documents are in line with these stringent obligations. **Transparency is key, but information overload should be avoided.**

Under the GDPR, new information must be provided to data subjects in a certain manner.

Fines and Penalties

The GDPR introduces a two-tiered system of **administrative fines:**

1. **€10,000,000** or, in the case of undertakings, **2%** of their total worldwide annual turnover, whichever is the higher.
2. **€20,000,000** or, in the case of undertakings, **4%** of their total worldwide annual turnover, whichever is the higher.

Apart from the administrative fines cited above, Member States may also impose **criminal sanctions** for specific infringements of data protection legislation. At present, the criminal sanctions applicable in Malta are limited in scope.

Moreover, data subjects may also claim **civil damages** for data protection infringements affecting their rights at law. The damages that may be claimed, even in Malta, may be both material and non-material meaning that **moral damages** (which previously existed only in very limited instances under Maltese law) may be claimed by data subjects in case of infringement of the GDPR.

Fines have been increased up to €20,000,000 or 4% of an entity's total worldwide annual turnover, whichever is the higher.

Privacy by Design and by Default and DPIAs

While controllers must continue to process personal data fairly, legally and transparently, the GDPR introduced the concept of **privacy by design** and by **default** whereby organisations must implement certain data protection principles (such as **data minimisation** and **processing only where necessary**) not only when the data are being processed but also at an early stage when the controller is determining the means for processing.

Controllers and processors are generally obliged to maintain a record of processing activities under their responsibility.

In some cases, generally when processing is likely to result in a high risk to the rights and freedoms of natural persons, organisations are legally mandated to carry out a **data protection impact assessment** or '**DPIA**'. Where the assessment reveals a **high risk**, prior consultation with the Information and Data Protection Commissioner will be required.

Under the GDPR, controllers must implement certain data protection principles as early as the moment when they are determining the means for processing and in some cases, controllers will be legally bound to carry out a data protection impact assessment.

New Data Subject Rights

New data subject rights include:

- The **'right to be forgotten'**: Controllers must erase all personal data of certain data subjects in certain specific circumstances (for example where the data are no longer needed for their original purpose or where the data subject revokes consent when no other lawful ground for processing exists); and

- The right to **'data portability'**: The data subject has the right to receive a copy of his/her personal data in a structured, commonly used and machine-readable format, and transfer his/her personal data from one controller to another.

Other data subject rights under the GDPR:

- Specified **time limits** within which controllers must reply to data subject requests for information;

- **Expanded rights** such as the **right of access, data restriction** and **objection to processing;** and

- Significantly **increased level of information** that must be provided to data subjects (see page 5). Such information must be provided in a **concise, transparent, intelligible** and **easily accessible** form, using **clear** and **plain language**.

Several new data subject rights have been introduced. These include the 'right to be forgotten' and the 'right to data portability'.

Maltese Implementing Measures

The Data Protection Act, 2018 (Chapter 586 of the Laws of Malta) (the 'Act') and the new subsidiary legislation issued under it, implement and further regulate the relevant provisions of the GDPR. The Act itself adopts a minimalist approach to GDPR implementation having only thirty-four (34) clauses, many of which relate to the role and functions of the local Information and Data Protection Commissioner and local enforcement procedures. The specific subsidiary legislation introduced under the Act as part of GDPR implementation are as follows:

- **Restriction of the Data Protection (Obligations and Rights) Regulations** (S.L. 586.09);

- **Processing of Data Concerning Health for Insurance Purposes Regulations** (S.L. 586.10); and

- **Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations** (S.L. 586.11).

Certain subsidiary laws issued under the previous legal regime (Chapter 440 of the Laws of Malta) have been renumbered and remain in force. Others have now been repealed.

The relevant Maltese law is the Data Protection Act, 2018 and the subsidiary laws issued under it.

What Else is Covered by the GDPR?

The GDPR clarifies and/or expands on several data protection principles and other issues that were already enshrined in the former legal regime (and are therefore not the focus of this document). These *include* the following:

- The general data protection principles including the core concepts of **lawfulness, fairness and transparency** when processing personal data;
- The **'storage limitation' principle** which limits **data retention periods** to **no longer than is necessary**;
- Rules regarding **direct marketing** which organisations must observe when trying to attract new customers or to offer promotions or marketing information to existing customers;
- Rules regarding the **content of data processing agreements** that must be entered into between the controller and the processor (now requiring considerably more detail);
- Special rules regulating **transfers to 'third countries'** not deemed to offer an adequate level of protection (including rules regarding **intra-group transfers** such as **binding corporate rules**);
- **Security measures** that must be implemented by both controllers and processors to protect personal data and *prevent* data breaches (the GDPR specifically cites, *inter alia*, encryption measures);
- Processing of **special categories of personal data** (formerly referred to as **sensitive personal data**) where the rules are more stringent;
- The **lawful grounds for processing** personal data **without consent**;
- Special rules regarding **personal data relating to children**; and
- Rules regarding **automated decision-making** (including **profiling**).

All the above require careful evaluation in view of new obligations under the GDPR.

What About ePrivacy?

At the time of publication of this document, the **proposed E-Privacy Regulation**, intended to repeal the EU's Privacy and E-Communications Directive (2002/58/EC) and all domestic laws implementing the same, (in Malta's case the 'Processing of Personal Data (Electronic Communications Sector), Regulations', subsidiary legislation 586.01) has not yet been finalised. Therefore, for the time being it is the above-cited Maltese law that would continue to apply. Once a finalised version of the E-Privacy Regulation is published, Mamo TCV will create an overview thereof and make it available on **www.mamotcv.com** and **www.gdprmalta.com**.

How Can Mamo TCV Advocates Help?

What we Offer

- **Comprehensive expert legal advisory services;**
- **On-site and/or online training of DPOs and other staff members;**
- **Drafting of privacy policies, notices, consent forms, T&Cs and other documents;**
- **Full legal representation in contentious matters and/or Commissioner investigations and/or court litigation;**
- **Carrying out of data protection impact assessments (DPIAs);**
- **On call assistance with data breaches and breach notification requirements.**

Mamo TCV Advocates is a leading law firm in the field of privacy law and, in particular, data protection legislation. Our clients range from world famous multinational IT companies to individual data subjects so we can provide you with practical advice regardless of the context. Whether you are uncertain of your rights when sharing personal data on social media or your corporate obligations in respect of your clients when moving your client data to the cloud or even your various duties as an employer, Mamo TCV has you covered.

In so far as the GDPR is concerned, we have carried out hundreds of GDPR compliance exercises and several training sessions for our diverse portfolio of clients and we have advised entities from many sectors on their unique data protection requirements. We also regularly assist clients with data breach reporting. In a number of instances, we even advised clients that notification was not legally required. In case of doubt, please feel free to contact us. **Urgent matters such as data breaches will be given top priority by our team of experts.**

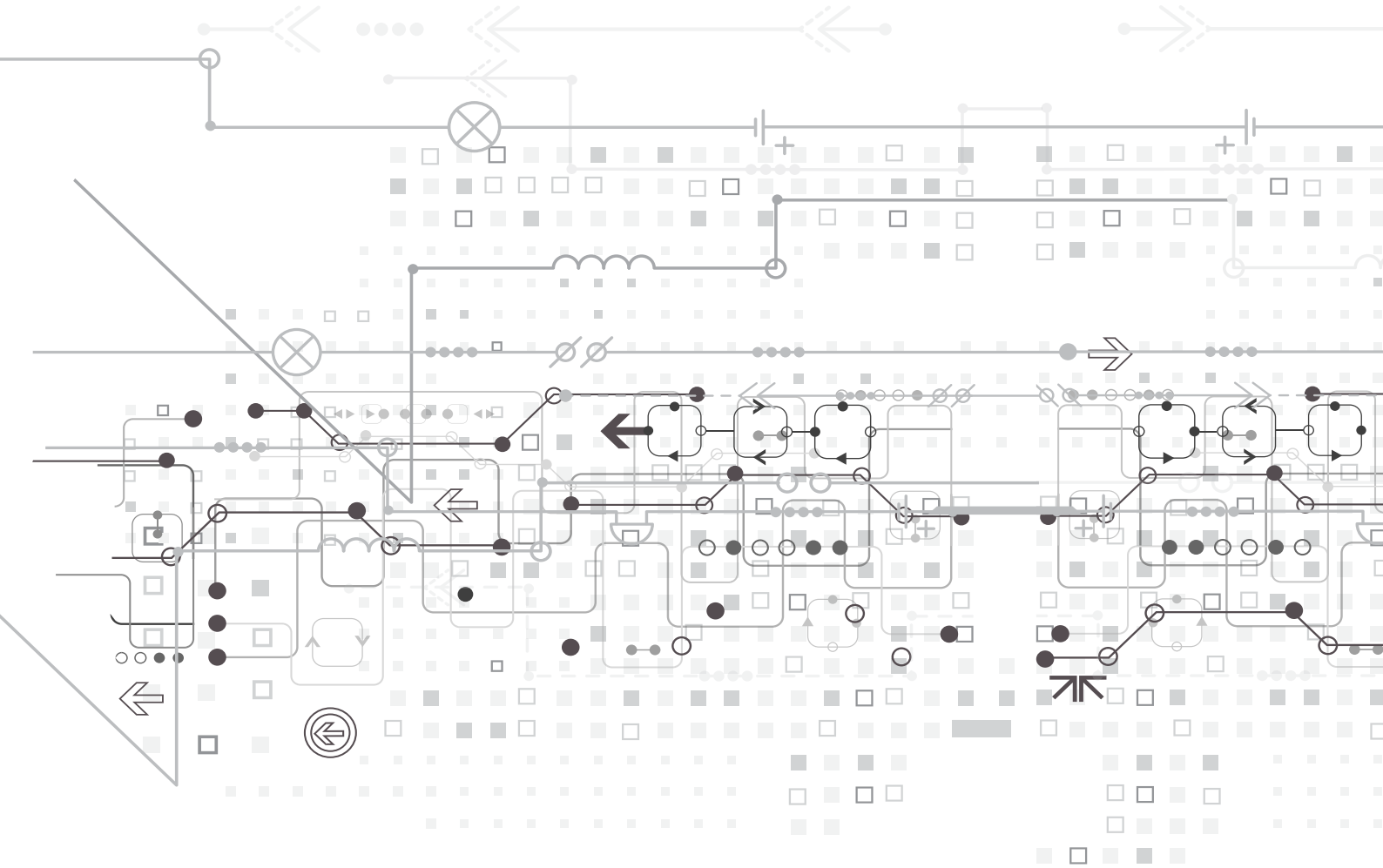
For more information on how Mamo TCV can help you, including providing you with a tailor-made memo outlining in more detail the various aspects of the GDPR itself and how this new legislation will impact you and your business here in Malta, please contact us by sending an email to **dataprotection@mamotcv.com.**

Should you wish to contact our data protection experts directly, please send an email to **Dr. Claude Micallef-Grimaud** (**claude.micallefgrimaud@mamotcv.com**) or **Dr. Antoine Camilleri** (**antoine.camilleri@mamotcv.com**).

The GDPR is here.

Are you compliant?

www.**gdprmalta**.com



MAMO TCV ADVOCATES

Palazzo Pietro Stiges
103 Strait Street
Valletta VLT 1436
Malta

T : (+356) 2540 3000
F : (+356) 2540 3300
W : www.mamotcv.com
E : dataprotection@mamotcv.com

MAMO TCV

ADVOCATES