

Data Subject Rights & Consent Under the GDPR

Dr Warren Ciantar
Senior Associate, Mamo TCV Advocates

warren.ciantar@mamotcv.com

21 Academy – DPO Course

| Malta | 18.04.2024 |





For a brief overview of the General Data Protection Regulation (GDPR) and updates regarding its implementation, please visit:

www.gdprmalta.com



MAMO TCV
ADVOCATES

Is your organisation GDPR compliant?

The GDPR or 'General Data Protection Regulation' (Regulation 2016/679/EU) is a new single EU law dealing with data protection that is intended to do away with the fragmented system that was previously in place and update laws across the EU that have not kept up with the digital age we live in. On 25 May 2018, as in the case of other EU Member States, the GDPR took effect in Malta. The new Data Protection Act, 2018 (Chapter 586 of the Laws of Malta) has also come into effect. Data controllers and processors had until this date to prepare for the various new, and in some cases, onerous obligations introduced by the GDPR.

[Mamo TCV GDPR Overview](#)

[DP Guidelines & Opinions](#)

[Data Protection Laws](#)

Maltese organisations (especially those processing large amounts of personal data) must take all necessary measures to ensure full compliance with this new law and this, as soon as possible.

Data Protection Opinions & Guidelines

[View all EDPB pages](#)

[EDPB Recommendations](#)

[EDPB Opinions](#)

Maltese Data Protection Guidelines

[Guidelines on the Collection of Employees' COVID-19 Vaccination Status](#)

[Guidelines for the Maltese Banking Industry](#)

[Guidelines for the Maltese Gaming Industry](#)

[Guidelines for Credit Reference Institutions](#)

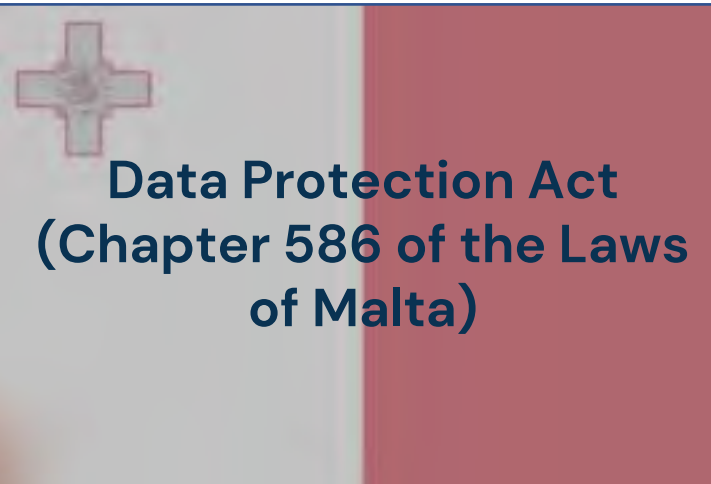
[Guidelines for Political Campaigning Purposes](#)

[Guidance Note on Cookies Consent Requirements](#)

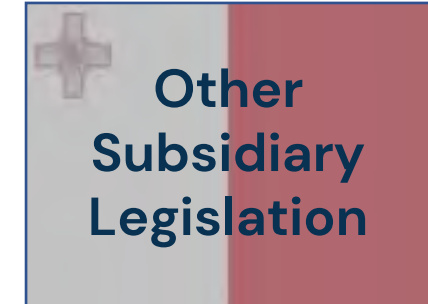
[Guidelines on Street Photography](#)



EU Regulation 2016/679
(GDPR)
(as of 25 MAY 2018)



Data Protection Act
(Chapter 586 of the Laws
of Malta)



Other
Subsidiary
Legislation

**“Everyone has the
right to the
protection of
personal data
concerning them”** Art
16 (TFEU)

The GDPR came into effect on 25 May 2018

- **Restriction of the data protection (obligations and rights) regulations**

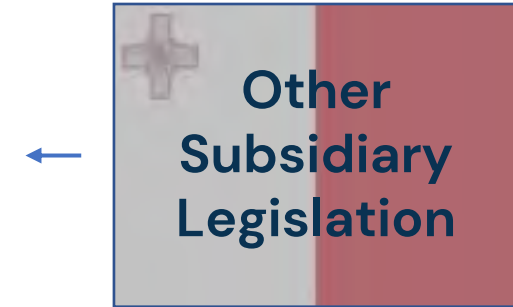
Applies restrictions to certain obligations and rights provided for in Article 23 of the GDPR.

- **Processing of data concerning health for insurance purposes regulations**

Introduces further conditions on the processing of data concerning health for insurance purposes pursuant to Article 9 of the Regulation.

- **Processing of child's personal data in relation to the offer of information society services**

Age of digital consent (re processing of personal data) has been lowered from **18 to 13**. **NB** – age of consent for valid contract formation in Malta remains 18.



The GDPR at a Glance

- ✓ Fines up to €20,000,000 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
- ✓ **Increased level of information** to be provided to data subjects
- ✓ More **stringent requirements** in controller–processor contracts
- ✓ Removal of the **general notification** requirement
- ✓ More stringent **consent** requirements
- ✓ New **data subject rights**

FAMILIARISE YOURSELF WITH KEY TERMINOLOGY

PERSONAL DATA &
SENSITIVE PERSONAL
DATA

DATA
CONTROLLER

PROCESSING

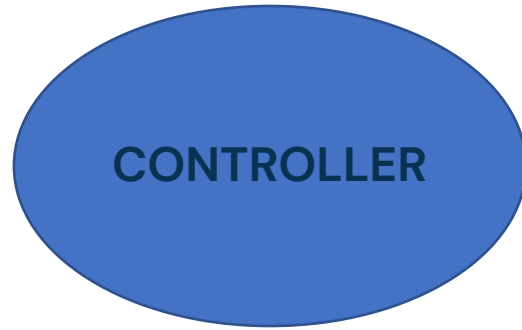
DATA
PROCESSOR

DATA
SUBJECT

DATA
PROTECTION
OFFICER



**ONLY
WHERE
PERSONAL
DATA ARE
PROCESSED**



DPA must be in place here



Sub Processing Agreement must be in place here (must reflect DPA between **Controller & Processor**)



- The entity that determines the purposes and means of the processing.
- The entity that is mainly responsible for processing of personal data.
- Don't be confused by the fact that *a controller also processes personal data*

Ex: - Schools (re students/teachers/parents)
- Banks (re clients/visitors)
- Website owners (re customers/users of website)
- All employers (re employees)

- **Sub Contractors** engaged by Controller to process personal data on Controller's behalf

Ex: - Outsourced Payroll/back-office service provider
- Web Developer
- Cloud Service Provider (if client is a Controller)

- **The Processor's Sub Contractors** engaged by **Processor** to assist with processing of personal data on Controller's behalf

Ex: - Provider of ancillary IT services
- Cloud Service Provider (if client is a **Processor**)

Requirements for Processing

Under **Art. 5** of GDPR, the **core data protection principles** can be summarised as follows:

- 1) **Lawfulness, Fairness and Transparency;**
- 2) **Purpose Limitation;**
- 3) **Data Minimisation;**
- 4) **Accuracy;**
- 5) **Storage Limitation;**
- 6) **Integrity and Confidentiality (Security Obligations);**
- 7) **Accountability**

- The 'Data Quality Principles' must always be adhered to in all cases (regardless of the legal basis for processing).
- Before ensuring that the other data quality principles are being complied with, a fundamental question must be asked:

"Is it lawful to process this personal data at all?"

"If so, on what ground(s)?"



Lawfulness of Processing (Article 6)

Non-Sensitive Personal Data may only be processed:

a) With consent of the data subject; or

- Consent must be unambiguous, freely given, specific and informed.
- GDPR makes it considerably harder to obtain valid consent (Art 7). Consent must also be provided by means of a **statement** or by a **clear and affirmative action**. Ex: **Pre-ticked boxes will no longer be permitted**.
- Controllers must now be able to demonstrate that consent has in fact been provided.
- Data Subject must be told that he/she has the right to *withdraw consent at any time*. "*It shall be as easy to withdraw as to give consent*".



Lawfulness of Processing (Article 6)

(Non-Sensitive) Personal Data may only be processed:

(Without Consent):

b) If processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

For example, personnel section should be able to process personal data without the necessity of consent for the purpose of complying with a contract of employment



Lawfulness of Processing (Article 6)

(Non-Sensitive) Personal Data may only be processed:

(Without Consent):

c) If processing is necessary for compliance with a legal obligation of the controller; or

For example, processing personal data to comply with Income Tax, Social Security or Employment law obligations.



Lawfulness of Processing (Article 6)

(Non-Sensitive) Personal Data may only be processed:

(Without Consent):

d) If processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; or

For example, disclosure of personal data to a hospital treating a casualty. **(NB** in case of sensitive personal data, a similar but stricter legal ground exists – as seen below).



Lawfulness of Processing (Article 6)

(Non-Sensitive) Personal Data may only be processed:

(Without Consent):

- e) ***If processing is necessary for the performance of a task carried out:**
- **In the public interest or**
 - **In the exercise of official authority vested in the controller; or**

For example, exercise of legal functions of a Government Department or in relation to the administration of justice.



Lawfulness of Processing (Article 6)

(Non-Sensitive) Personal Data may only be processed:

(Without Consent):

- f) *If processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (particularly children).

A general clause which may be used in absence of consent (NOT by public authorities).

Must be examined on a **case-by-case basis** & should be re-evaluated in terms of the GDPR.



CONSENT

Consent Under the GDPR

One of the lawful grounds to process **non-sensitive personal** data under **Art. 6**

One of the lawful grounds to process **sensitive personal data** under **Art. 9**

Examples where consent can be used in specific processing operations:

One of the grounds for carrying out direct marketing

Necessary for using non-essential 'cookies'

One of the grounds for implementing automated decision-making (no human intervention) – Art 22

Consent Under the GDPR

- ▶ Article 4(11) of the GDPR defines consent as:

*“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.”*

See Article 29 Working Party/EDPB **Guidelines on Consent** (10th April 2018)

Conditions for Consent (Art 7, GDPR)

1. Where processing is based on consent, the controller shall be **able to demonstrate** that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is **clearly distinguishable from the other matters**, in an intelligible and easily accessible form, using **clear and plain language**. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. **The data subject shall have the right to withdraw his or her consent at any time.** The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. **It shall be as easy to withdraw as to give consent.**
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Elements of Valid Consent:

- Article 4(11) of the GDPR stipulates that consent of the data subject means any:
 - freely given,
 - specific,
 - informed and
 - unambiguous



Consent: “Freely Given”

- There must be a ‘real choice’.
- Being compelled to give consent will invalidate that consent.
- Being unable to refuse or withdraw consent without detriment is not ‘freely given consent’.
- No coercion, deception, intimidation or significant detrimental effect in case of a ‘No’.
- Imbalance between controller and data subject to be taken into account (example: Public Authorities vs Citizens and Employers vs Employees).

Consent: “Freely Given”

Article 7(4): *When assessing whether consent is freely given, utmost account shall be taken of whether, **inter alia**, the performance of a contract, including the provision of a service, is **conditional** on consent to the processing of personal data that is not necessary for the performance of that contract.*

Tying or **bundling** consent for something (ex. direct marketing) with a contract/service where that consent is not necessary = invalid consent.

Undue pressure/influence on a data subject preventing data subject from exercising **free will** shall render consent invalid.

Purpose of the processing cannot be disguised.

If something is **necessary for the performance of a contract** (to be interpreted strictly), that legal ground should be invoked NOT consent. The two should not be merged.

Consent: “Freely Given”

EDPB Example:

A public school asks students for consent to use their photographs in a printed student magazine.

Q. Can consent be said to be ‘freely given’ here?

Yes. Consent in these situations would be a genuine choice **as long as** students will not be denied education or services and could refuse the use of these photographs without any detriment.

NB – in Malta, age of consent in education sector is 16 (S.L. 586.07)

Consent: “Freely Given”

EDPB Example:

A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services.

Q. Can consent be said to be freely given here?

No. If the customer’s refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.

Yes. If the customer’s refusal to consent to this processing purpose would not lead to any such **detrimental effect** on him/her (i.e. if there is a real choice/exercise of free will).

Consent: “Freely Given”

Granularity:

Recital 32, GDPR: *“Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them”.*

I.e. Separate consent must be obtained for multiple processing operations having different purposes.

Same rules re ‘free will’, ‘real choices’ etc. apply to each of these different processing operations.

Ex: Consent is collected to send direct marketing AND to share personal data with affiliates. You would need separate consent here (for the **two separate purposes**).

NB – Consent must also be ‘specific’

Elements of Valid Consent:

- Article 4(11) of the GDPR stipulates that consent of the data subject means any:
 - **freely given,**
 - **specific,**
 - **informed** and
 - **unambiguous**



Consent: “Specific”

To comply with the element of 'specific' the controller must apply:

- (i) **Purpose specification** as a safeguard against ‘function creep’,
- (ii) **Granularity** in consent requests, and
- (iii) Clear separation of **information** related to obtaining consent for data processing activities from information about other matters.

No ‘open-ended’ consent.

Function creep = blurring or widening of purposes for processing after data subject agreed to initial collection (leading to unanticipated use of Personal Data + loss of control over Personal Data)

Consent: “Specific”

EDPB Example:

A cable TV network collects subscribers’ personal data, based on their consent, to present them with personal suggestions for new shows/movies they might be interested in based on their viewing habits. After a while, the TV network decides it would like to enable third parties to send (or display) targeted advertising on the basis of the subscriber’s viewing habits.

Q. Is new consent needed for this new purpose or was initial consent specific enough?

EDPB Answer: (Yes) “Given this new purpose, new consent is needed”.

Remember, no open-ended consent

Elements of Valid Consent:

- Article 4(11) of the GDPR stipulates that consent of the data subject means any:
 - **freely given,**
 - **specific,**
 - **informed** and
 - **unambiguous**



Consent: “Informed”

Data subjects must be given all the information they need to be able to take an informed decision.

This includes information regarding their rights (especially the right to withdraw consent at any time).

Linked with the ‘transparency’ principle (which must be applied in any case – even where other grounds are relied on). See Art. 13/14

Without all necessary information being provided (in clear and plain language), consent would not be valid.

Consent: “Informed”

EDPB stated that in so far as consent is concerned the following is the **MINIMUM** information that must be provided to the data subject:

- (i) the controller’s identity (including joint controllers),
- (ii) the purpose of each of the processing operations for which consent is sought,
- (iii) what (type of) data will be collected and used,
- (iv) the existence of the right to withdraw consent,
- (v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and
- (vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.

Consent: “Informed”

How should you provide this information to data subjects?

GDPR is silent. Important thing is to ensure that this information is actually provided (and to have proof of this).

Remember Article 7(2):

*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an **intelligible** and **easily accessible** form, using **clear and plain language**. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

You shouldn't have to be a lawyer to understand data protection notices/policies!

Consent: “Informed”

There are specific EDPB guidelines on ‘transparency’ (re obligations under Art. 13 and 14).

The guidelines emphasise the importance of **LAYERED NOTICES** (no scrolling through long notices).

In non-digital notices, conciseness is key (with easy access to full privacy policy – even in paper form).

NO HIDDEN CONDITIONS

Consent: “Informed”

EDPB Example:

A company engages in data processing on the basis of consent. The company uses a layered privacy notice that includes a consent request. The company discloses all basic details of the controller and the data processing activities envisaged. However, the company does not indicate how their data protection officer can be contacted in the first information layer of the notice.

Q. Is consent ‘informed’ here?

Answer: **Yes.** For the purposes of having a **valid lawful basis as meant in Article 6**, this controller obtained valid “informed” consent, even when the contact details of the data protection officer have not been communicated to the data subject (in the first information layer), pursuant to Article 13(1)(b) or 14(1)(b) GDPR.

NB – this does not mean that you are GDPR compliant (Art. 13/14 needs to be complied with in any case)

Consent: “Informed” - REMINDER

EDPB states that in so far as consent is concerned the following is the **MINIMUM** information that must be provided to the data subject:

- (i) the controller’s identity (including joint controllers),
- (ii) the purpose of each of the processing operations for which consent is sought,
- (iii) what (type of) data will be collected and used,
- (iv) the existence of the right to withdraw consent,
- (v) information about the use of the data for automated decision-making in accordance with Article 22 (2)(c) where relevant, and
- (vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46.

Elements of Valid Consent:

- Article 4(11) of the GDPR stipulates that consent of the data subject means any:
 - **freely given,**
 - **specific,**
 - **informed** and
 - **unambiguous**



Consent: “Unambiguous”

Remember Article 4(11):

*“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.”*

It must be obvious that the data subject has given (valid) consent.

- Ambiguity should be avoided
- Silence cannot be interpreted as consent
- NO PRE-TICKED OPT-IN BOXES (when requiring consent)
- Recorded vocal consent is valid (if all necessary information is provided)

Consent flow should be designed for the needs of each organisation (not too disruptive but valid)

Consent: “Unambiguous”

Whatever the means of obtaining consent (swipe left, gestures, etc.), the **QUESTIONS** being asked must be presented in a manner that will likely be read by data subjects

NB – consent must be obtained BEFORE processing commences. This is implied from article 4, GDPR.

Fresh consent should be obtained at ‘**appropriate intervals**’ (certainly if purpose changes).

Elements of Valid Consent:

- Article 4(11) of the GDPR stipulates that consent of the data subject means any:
 - **freely given,**
 - **specific,**
 - **Informed and**
 - **unambiguous**



When is *Explicit* consent required?

When there is added risk to processing:

- ▶ When processing SENSITIVE personal data (special categories of data)
- ▶ Transfers to third countries where there is no adequacy decision or adequate safeguards
- ▶ Decision-making taken solely by automated means (no human intervention)

How can explicit consent be provided?

- ▶ Written, signed, statement (not always practical)
- ▶ Filling an electronic form
- ▶ Sending an email
- ▶ Uploading a scanned document carrying a signature
- ▶ Electronic signatures

Oral statements can also be deemed 'explicit' but difficult in terms of record keeping obligations.

Two stage verification is strongly encouraged (especially where sensitive personal data is concerned – ex health data).

Acceptable YES NO check boxes: **"I, hereby, consent to the processing of my data"** (all information must be provided + other requirements)

Other Consent Requirements

“Demonstrate Consent”

Article 7(1), GDPR:

Where processing is based on consent, **the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.**

- ▶ Up to controller to determine how to do this (Without collecting further information other than what is necessary)
- ▶ Burden of proof is on the Data Controller
- ▶ **Proof of consent** (plus information actually given to data subject) must be kept for as long as processing based on consent lasts + thereafter for as long as legally obliged OR necessary for establishment, exercise or defence of legal claims.
- ▶ EDPB recommends REFRESHING CONSENT at ‘appropriate intervals’

Other Consent Requirements

“Withdrawal of Consent”

Article 7(3), GDPR:

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. **It shall be as easy to withdraw as to give consent.**

If giving consent provided via a ‘mouse-click’, it must be withdrawable in a similarly easy manner (not necessarily a ‘mouse-click’).

Withdrawal should be without detriment (see ‘freely given’ requirement) and free of charge (no lowering of service levels etc.)

Other Consent Requirements

“Withdrawal of Consent”

- ▶ Before obtaining consent, the data subject must clearly be told that he/she has the right to withdraw consent at any time.
- ▶ Processing pre withdrawal remains lawful but processing must stop UNLESS there is another valid ground (that was communicated to the data subject) – ex ‘further storage’.
- ▶ To avoid pitfalls, the key is TRANSPARENCY. Tell data subjects if there are more grounds that apply in advance.
 - ▶ NO HIDDEN LEGAL GROUNDS.
 - ▶ No SILENT MIGRATION from consent to another ground.
- ▶ Even if there is no request to ‘erase data’ (see right to be forgotten), controllers must still determine appropriateness of retaining data after consent has been withdrawn.

Other Consent Requirements

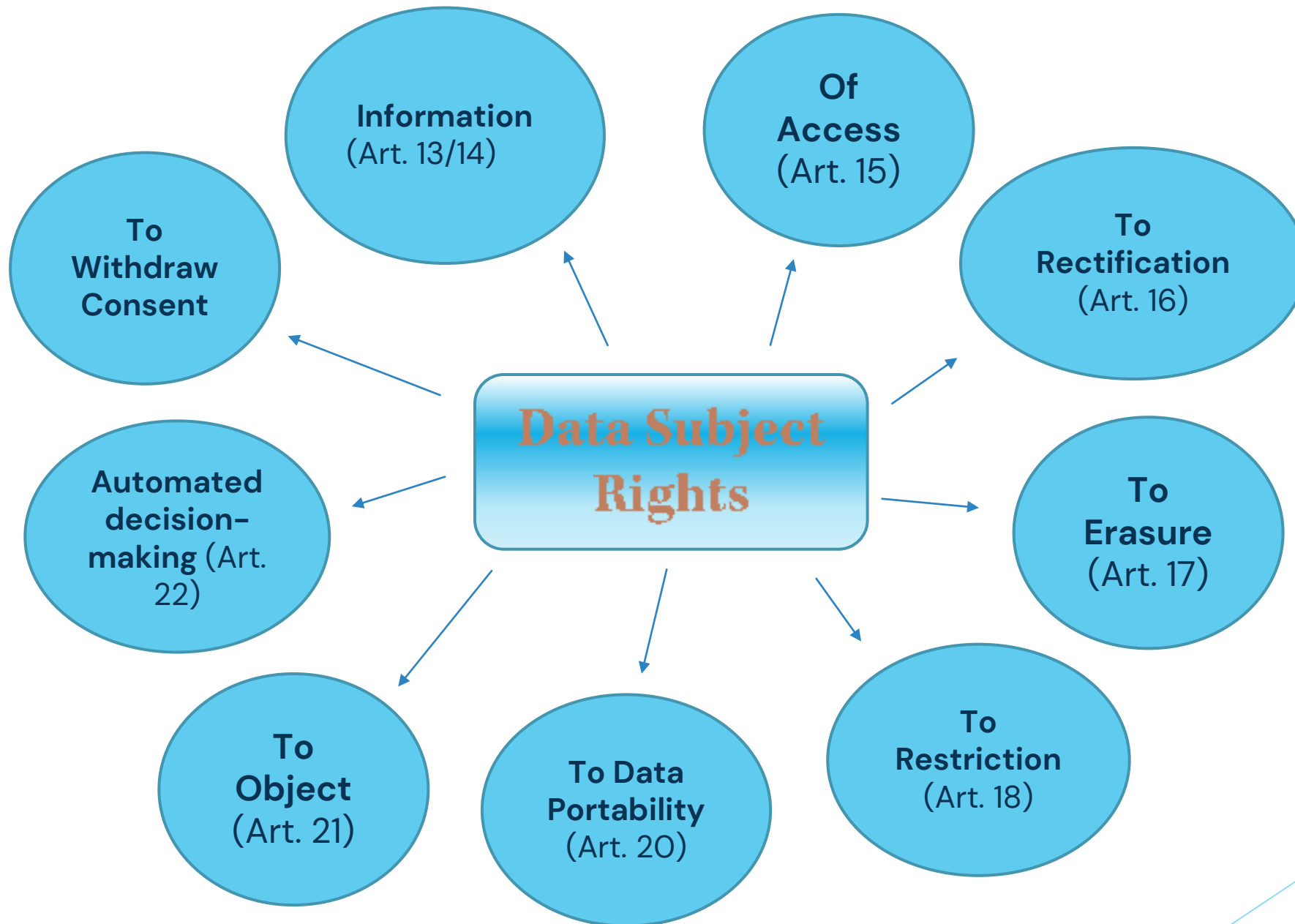
Consent of children. Article 8, GDPR

- ▶ In Malta, age of digital consent is now 13 (previously 18).
- ▶ This means that parental consent is required for any minors using services online.
- ▶ **NB** age of consent in education sector (586.09) = 16.

[Read EDPB Guidelines on Consent – section 7.2 on Scientific Research](#)

A close-up photograph of a white ceramic coffee cup filled with dark coffee, resting on a matching white saucer. A silver spoon is tucked behind the cup. The background is softly blurred, showing what appears to be a tray of pastries or bread. In the upper left corner, there is a dark circular graphic with a double-line border containing the text "Break Time!".

**Break
Time!**



General Rules Regarding Rights (Art.12)

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a **concise, transparent, intelligible** and **easily accessible** form, using **clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the **controller shall not refuse to act** on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within **one month** of receipt of the request. That period may be extended by **two further months** where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. **If the controller does not take action** on the request of the data subject, the **controller shall inform the data subject** without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

General Rules Regarding Rights (Art.12)

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided **free of charge**. Where requests from a data subject are **manifestly unfounded** or **excessive**, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the **controller may request the provision of additional information necessary to confirm the identity of the data subject**.

Information to Data Subject (Art. 13)

See EDPB Guidelines on Transparency

The Data Subject is entitled to certain information from the Controller (with or without a request):

GDPR adds information that must be provided to data subject – (ex. **period of retention of data (or criteria used) + details of DPO + legal basis for processing (and if it's legit. Interests, what these are) + ability to withdraw any consent given + existence of automated processing**). Similar in case data is collected from other sources (**Art. 14**) + **source of data and categories of personal data concerned**.

NB – The information provided to data subjects must be **concise, transparent, intelligible** and **easily accessible** using **clear and plain language** (**Art. 12**).



Information to Data Subject (Art. 13)

See EDPB Guidelines on Transparency



The Right to Object to Processing (Art. 21)

1. The data subject shall have the right to object, **on grounds relating to his or her particular situation**, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.



The Right of Access (Art. 15)

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not **personal data** concerning him or her [regardless of whether data subject gave this to controller] are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) **the right to lodge a complaint with a supervisory authority;**
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.



The Right of Access (Art. 15)

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide **a copy** of the personal data undergoing processing. For any **further copies** requested by the data subject, the controller may charge a **reasonable fee** based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. **The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others. CHECK YOUR IP Limits**

NB - Requested information must be given within **one month** from receiving request (can be extended to two months in some cases)

The GDPR clarifies that the right of access exists to allow data subjects to be aware of and can verify the lawfulness of the processing (Recital 63).

The Right of Access (Art. 15)

Some Tips on How to Prepare for SARs (and/or data portability requests)

- **Data Mapping**. Know what you have and where your data is to quickly and efficiently locate information in case of a request. If you haven't already started, start with high priority areas – HR, marketing, legal etc.
- **Plan ahead for valid/invalid requests**. Have template replies ready one way or the other. Ex. From data mapping exercise, you should be able to quickly check whether the request is coming from someone not associated with your organisation. **Remember to authenticate identity of individuals** requesting access.
 - **Also, create internal rules to know what to give and what not to give (ex certain inferred data, internal notes etc.).**



The Right of Access (Art. 15)

Some Tips on How to Prepare for SARs (and/or data portability requests)

- Use technology to help with common requests (portals, 'download your data' etc.) – 'self service' system (if possible).
Ex. Remote access (Recital 63)
- Update retention policies and have this information readily available.
- Train your Staff & organisation – what GDPR is, what SARs are. 'Is this a SAR or not' (even if not specifically described as such!)
- Carry out regular legal and technical audits

The Right to Data Portability Art. 20 (GDPR)

See EDPB Guidelines on the Right to Data Portability .

1. The data subject shall have the right to receive the personal data concerning him or her, **which he or she has provided to a controller**, in a **structured, commonly used and machine-readable format** and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
 - (a) the **processing is based on consent** pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); **AND**
 - (b) the **processing is carried out by automated means** [NB not solely].
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, **where technically feasible**.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17 [the right to be forgotten]. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. [i.e. No automatic right to erasure]
4. The right referred to in paragraph 1 **shall not adversely affect the rights and freedoms of others**.

The Right to Data Portability Art. 20 (GDPR)

Intended to facilitate switching between service providers

Closely related to the Right of Access but more conditions for it to apply.

– **A Right to Receive Personal Data** (e.g. contact lists from webmail applications, information regarding purchases using different loyalty cards etc.) **and be able to reuse that data.**

– **A Right to Have Personal Data Transmitted Between Controllers** – (where technically feasible). **NB** – controllers are encouraged to develop interoperable formats.

Ex. 1: Titles of books purchases from an online bookstore

Ex. 2: Songs listened to via a streaming service



The Right to Data Portability Art. 20 (GDPR)

How must portable data be provided?

- **Format:** not specifically defined but law refers to a “*structured, commonly used and machine-readable format*”

These are minimum requirements intended to facilitate “interoperability”

If there are no industry standards, EDPB encourages open formats: XML, JSON, CSV etc. A pdf copy of a user’s inbox would not facilitate **re-use** so it would probably not be sufficient.

“without hindrance” but at the same time “where technically feasible”.



The Right to Data Portability Art. 20 (GDPR)

Other Points

- All necessary information to be provided
- Tools should be implemented to allow data subject to select relevant data they wish to receive.
- Controllers should identify data subject before proceeding (but not use this as an excuse to reject request). Authentication procedures are encouraged by the EDPB (to strongly ascertain identity). **NB – NO EXCESSIVE DEMANDS**
 - Username and passwords can suffice
- Time limits must be respected (no silence)
- **Security measures to protect data must be in place** (ex. Ensuring data is sent to the correct entities).



Right to Rectification (Art. 16)

*The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate **personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have **the right to have incomplete personal data completed**, including by means of providing a supplementary statement.*

NB – this is linked to the principle of ‘Accuracy of Personal Data’

Controller may verify accuracy before rectifying the personal data (if possible)

The Right to Be Forgotten (Art. 17)

1. The data subject shall have the right to obtain from the controller the erasure of personal data **concerning him or her without undue delay** and the controller shall have the obligation to erase personal data without undue delay where **one** of the following grounds applies:

(a) **the personal data are no longer necessary** in relation to the purposes for which they were collected or otherwise processed;

(b) **the data subject withdraws consent** on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) **the data subject objects to the processing** pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) **the personal data have been unlawfully processed;**

(e) **the personal data have to be erased for compliance with a legal obligation** in Union or Member State law to which the controller is subject;

(f) **the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).**



The Right to Be Forgotten (Art. 17)

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take **reasonable steps**, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Ex. Companies may need to inform search engines to remove certain information (ex cached data) that has been erased from the companies' website.



The Right to Be Forgotten (Art. 17)

The Right to Be forgotten on the basis of any one of these grounds (and the obligation to inform other controllers) **WILL NOT APPLY** if the Controller can show that retention/processing is **necessary**:

(a) for exercising the right of **freedom of expression and information**;

(b) for **compliance with a legal obligation** which requires processing by Union or Member State law to which the controller is subject **or** for the **performance of a task carried out in the public interest or in the exercise of official authority** vested in the controller;

(c) for reasons of **public interest** in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the **establishment, exercise or defence of legal claims**.



Right to Restriction of Processing (Art. 18)

What Does 'Restriction of Processing' Mean?

Article 4(3):

*'restriction of processing' means the marking of **stored personal data** with the aim of limiting their processing in the future'*

Recital 67:

Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

Right to Restriction of Processing (Art. 18)

1. The data subject shall have the right to obtain from the controller **restriction of processing** where **one** of the following applies:
 - (a) the **accuracy of the personal data is contested** by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
 - (b) the **processing is unlawful** and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
 - (c) the **controller no longer needs the personal data** for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
 - (d) the **data subject has objected to processing pursuant to Article 21(1)** pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, **with the exception of storage**, only be processed **with the data subject's consent** **or** for the establishment, exercise **or** defence of legal claims **or** for the protection of the rights of another natural or legal person **or** for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Automated Individual Decision-Making, Including Profiling (Art. 22)

See EDPB Guidelines on Automated Decision-Making.

1. The data subject shall have the right not to be subject to a decision based **solely** on automated processing, including profiling, **which produces legal effects** concerning him or her **or similarly significantly affects** him or her.
2. Paragraph 1 shall not apply if the decision:
 - (a) is **necessary for** entering into, or **performance of, a contract** between the data subject and a data controller; or
 - (b) is **authorised by Union or Member State law** to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's **explicit consent**.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement **suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests, *at least* **the right to obtain human intervention** on the part of the controller, **[the right] to express his or her point of view** and **[the right] to contest the decision**. *NB – information must be given (on logic etc.) regardless. This helps data subject exercise rights.*
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Top Priorities

Update all information provided to data subjects (e.g. privacy policies);

DPO training;

Enter into GDPR-compliant Data Processing Agreements;

Update contracts of employment/HR notices;

Make sure marketing practices are GDPR compliant (opt-in? opt-out?);

Prepare for the various data subject rights (e.g. SARs);

Prepare for data breaches (DPO, internal procedures, templates);

Ensure that all data quality principles are in place (lawfulness, retention periods etc.);

Check your record keeping obligations

Carry out an IT audit/gap analysis (are security measures up to scratch?).

Recent Decisions



DPG Media - Netherlands SA - 14th January 2022

- Dutch data protection authority imposed a fine of €525,000 on DPG Media
- The company was forcing people who wanted to exercise their right of access or erasure to first upload proof of identity - a copy of an identity document - which contains far more personal data than required.
- This was deemed excessive in the circumstances. The company now sends a verification email instead to establish identity of the person making the request.
- Copies of ID cards and passports are a source of great risk, if they fall into the wrong hands they could lead to identity theft/fraud and have severe consequences for the person to whom the data belongs. Avoid keeping these copies wherever possible.

Maltapost plc vs IDPC - Court of Appeal - 5th October 2018

- In general, a retention period for CCTV footage of 7 days shall be applicable, with exceptions allowed only in exceptional circumstances
- In this instance, a special concession of 20 days was granted to Maltapost's "Data Management System Area"
- Malta Banking Guidelines provide for extended retention periods of CCTV footage for banks
- Where CCTV footage is relevant to an investigation, a copy of the relevant extract of such footage may be retained until such investigation is concluded.

Thank You for Your Attention

Mamo TCV Advocates

Palazzo Pietro Stiges
103, Strait Street
Valletta VLT1436
Malta

T: (+356) 25 403 000

F: (+356) 21 244 291

E: info@mamotcv.com

www.mamotcv.com

www.gdprmalta.com