Remote Managing your Employees – the Legal Implications

Dr Christine Calleja

Dr Warren Ciantar

19.10.22

MAMO TCV ADVOCATES

www.21Academy.education

1. Teleworking

2. Health and Safety

3. Data Protection

4. Remote Working

MAMO TCV
ADVOCATES

Is Working from Home a Legal Right?

- Generally – no.
- Work Life Balance for Parents and Carers Regulations – right to request flexible working arrangements for caring purposes.
- Only workers with children up to age of 8 years and carers.
- Can request to return to normal patters before expiration of agreed period – employer can refuse.
- Flexible working arrangements – remote working / work on reduced hours / flexitime.
- 2 working weeks for employer to reply – must give reasons for refusal or postponement.

MAMO TCV
ADVOCATES

What are the trends of home working?

- Studies of European Commission:
- Before 2020 – 5% of people in the EU worked regularly from home.
- In 2020 – 40% started teleworking fulltime.
- Most common – highly skilled workers such as IT professionals.
- Regional differences – more common in northern Europe – more jobs available in sectors able to telework and cultural differences.

Pros and Cons of Telework

- Pros:
- Less commute time;
- More work-life balance;
- Increased productivity;
- Reduced work related expenses – food and clothing.

- Cons:
- People work longer hours and take fewer breaks;
- Social Isolation.
- Women finding it more difficult.
- No separation between work and home.

MAMO TCV
ADVOCATES

What can the employer do to address issues of teleworking?

MAMO TCV
ADVOCATES

Suggestions…

- Encourage employees to ask for help if required.
- Building interpersonal relationships with employees and regularly check in with them.
- Encourage employees to take breaks regularly and stay connected with colleagues.
- Provide contact details for external mental health support services.

Working in the Metaverse?

- https://www.youtube.com/watch?v=uVEALvpoiMQ
- https://www.youtube.com/watch?v=hw03I8tb7Ko

How does the law regulate remote working?

- Telework National Standard Order S.L. 452.104

- Telework – *'a form of organising and, or performing work, using information technology, in the context of an employment contract or relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis'.*

MAMO TCV
ADVOCATES

Telework National Standard Order

- Telework – agreement in the contract or by separate agreement.
- If not agreed in contract – either party may propose and other may refuse.
- Right to terminate telework by both parties – first 2 months – 3 days' notice in writing / after 2 months – 2 weeks' notice unless different agreement is reached.

MAMO TCV
ADVOCATES

Telework National Standard Order

- Agreement must be in writing and:

- Contain information required in the Information to Employees Regulations and info on the following:

- Location for telework;
- Equipment to be used;
- Amount of working time at workplace and at place of telework;
- Schedule by which employee will perform telework;

Telework National Standard Order

- Description of work to be performed;
- Department and immediate superior;
- Any provisions relating to monitoring;
- Notice of termination of teleworking;
- Right of revertability to return to place of work.

Telework National Standard Order

- During telework – employee is to enjoy same rights as provided for under Chapter 452 or collective agreement AND right of access and rights to participate in training.
- Equipment to provide the telework – employer responsible to provide, install and maintain necessary equipment unless otherwise provided.
- Employer is to cover costs of communication directly caused by telework.

Occupational Health and Safety

- What obligations exist on the employer in the case of teleworking?
- Obligation to inspect vs obligation to inform.
- Need for causal link between work and injury.
- https://www.washingtonpost.com/world/2021/12/10/work-home-injury-germany/?fbclid=IwAR0mcMNBes7gbtrpt82qvTOFrHMLBvvqkyAQ1QbUT56G7AQZ01zoKNOQgVc

Stress at work – an OHSA Consideration?

- UK's HSE's definition of stress:

"The reaction people have to excessive demands or pressures, arising when people try to cope with tasks, responsibilities or other types of pressure connected with their job, but find difficulty, strain or worry in doing so."

MAMO TCV
ADVOCATES

Stress at work – an OHSA Consideration?

- Health and safety – includes obligation to ensure there are no excessive levels of stress;
- Sources – excessive work; harassment; bullying.
- Problems – very subjective + low chances of authorities to intervene;
- Rarely form part of risk assessment;
- Usually tied to cases of constructive dismissal.
- Can lead to phycological disorders – cases of damages.

Organisation of Working Time Regulations

- Directive 2003/88/EC (the Working Time Directive) → aim at providing minimum standards common to MS to protect workers from health and safety risks associated with excessive or inappropriate working hours, and with inadequate time for rest and recovery from work.

- Limit to weekly working hours / Rest Breaks / Minimum Daily Rest / Minimum Weekly Rest / Paid Annual Leave / Protection in case of Night Work.

MAMO TCV
ADVOCATES

Organisation of Working Time Regulations

- Daily Rest – 11 consecutive hours per 24hr period;
- Rest Break – At least 15mins if working day longer than 6hrs;
- Weekly Rest – 24hrs for every 7 days;
- Maximum Average Working Time – 48hrs per week including overtime (opt-out clauses);
- Annual leave – at least 27 days per year / provisions on carrying forward of leave;
- Night work – hours of work not to exceed 8hrs in every 24hr period.

MAMO TCV
ADVOCATES

Employees working remotely from abroad

- Jurisdiction in case of disputes:
- Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

- If an employer is not domiciled in a MS but has a branch, agency or other establishment in a MS – employer deemed to be domiciled in that MS.

Jurisdiction cont.

- Employed domiciled in a MS may be sued:
- In the courts of MS where he is domiciled OR in another MS from where the employee habitually carries out his work or the last place from where he did so OR if he does not habitually carry out work in one country, where the business which engaged him is situated.
- Employer not domiciled in a MS – can be sued in country from where the employee carries out his work or where the business is situated.

Jurisdiction cont.

- Employer can only sue the employee in the courts of the Member State where the employee is domiciled.
- Employer can however bring a counter claim in the same court hearing the original claim.
- Can only depart from these provisions by agreement:
- 1. Entered into AFTER the dispute has arisen; OR
- 2. Allows the employee to bring proceedings in other courts.

Choice of Law

- Which law applies to employment contracts?

- REGULATION (EC) No 593/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 June 2008 on the law applicable to contractual obligations (Rome I)

Choice of Law

- *1. An individual employment contract shall be governed by the law chosen by the parties in accordance with Article 3. Such a choice of law may not, however, have the result of depriving the employee of the protection afforded to him by provisions that cannot be derogated from by agreement under the law that, in the absence of choice, would have been applicable pursuant to paragraphs 2, 3 and 4 of this Article.*

Choice of Law

- *2. To the extent that the law applicable to the individual employment contract has not been chosen by the parties, the contract shall be governed by the law of the country in which or, failing that, from which the employee habitually carries out his work in performance of the contract. The country where the work is habitually carried out shall not be deemed to have changed if he is temporarily employed in another country.*

Choice of Law

- *3. Where the law applicable cannot be determined pursuant to paragraph 2, the contract shall be governed by the law of the country where the place of business through which the employee was engaged is situated.*

- *4. Where it appears from the circumstances as a whole that the contract is more closely connected with a country other than that indicated in paragraphs 2 or 3, the law of that other country shall apply.*

MAMO TCV
ADVOCATES

Issues of Income Tax and Social Security

- What is the situation in Malta?
- Social Security - paid by employed persons - Class 1 Contributions and are paid by direct deductions from the same employees' wages/salary. In a normal case scenario, an equivalent rate paid or deducted from the employee's wage/salary, is also paid by the employer.
- The Social Security Contribution rate due is based on earning derived from the Basic Weekly Wage.
- Both employer and employee's share of Class 1 Social Security Contributions are paid to the Commissioner of Inland Revenue in monthly payments by the employer.
- What if the employee is not resident in Malta?

MAMO TCV
ADVOCATES

Social Security

- Persons employed under a contract of service outside Malta, but who retain their ordinary residence in Malta, may request the Director – DSS to pay Class 1 (Employed person) contributions instead of Class 2 contributions.

- Article 13(1) provides that no social security contribution shall be payable by or on behalf of the employer. Following a request, the Department issues Social Security Contribution bills to cover the period of foreign employment as requested to the Director – Department of Social Security.

- Although equivalent to Class 1 contributions, Social Security Contributions under Article 13(1) are paid in the same manner as Self-Occupied Class 2 contributions. That is, to the Commissioner of Inland Revenue every 4 months; namely in April, August and December respectively, or until the same employment conditions continue to apply.

- Exceptions made by IRD – allow employer to register in Malta without having a physical presence in Malta.

- Employer and employee to check – is there an equivalent in the jurisdiction where the employee is currently residing?

Social Security Principles in the EU

1. You are covered by the legislation of one country at a time so you only pay contributions in one country. The decision on which country's legislation applies to you will be made by the social security institutions.
2. You have the same rights and obligations as the nationals of the country where you are covered. This is known as the principle of equal treatment or non-discrimination.
3. When you claim a benefit, your previous periods of insurance, work or residence in other countries are taken into account if necessary.
4. If you are entitled to a cash benefit from one country, you may generally receive it even if you are living in a different country. This is known as the principle of exportability.

MAMO TCV
ADVOCATES

Which rules apply?

- Employee is subject to the legislation of the country where employee actually work as an employed or a self-employed person. It doesn't matter where employee lives or where employer is based.

- If employee works in a different EU country from the one where employee lives and employee returns to country of residence daily, or at least once a week, employee is a cross-border worker (so-called "frontier worker"). The country where employee works is responsible for social security benefits.

MAMO TCV
ADVOCATES

Which rules apply?

- If you pursue a substantial part of your activity, at least 25%, in your country of residence, you will be covered by the legislation of that country.
- If you don't pursue a substantial part of your activity in your country of residence, you will be covered by the legislation of the country where the registered office or place of business of your employer is situated.
- If you work for several employers, whose registered offices are in different countries, you will be covered by the legislation of your country of residence; even if you don't pursue a substantial part of your activity there.
- If you are self-employed and you don't pursue a substantial part of your activity in your country of residence, you will be covered by the legislation of the country where the centre of interest of your activities is situated.
- If you pursue an employed and a self-employed activity in different countries, you will be insured in the country where you are employed.

MAMO TCV
ADVOCATES

Income Tax

- Maltese rules – Malta has the right to tax:
- Income and capital gains arising in Malta;
- Income and taxable capital gains arising abroad to persons who are ordinarily resident and domiciled in Malta;
- Foreign source income derived by persons who are ordinarily resident in Malta but not domiciled in Malta which is received in Malta;
- Foreign source income derived by persons who are domiciled in Malta but not ordinarily resident in Malta which is received in Malta.

Handling Grievances and Disciplinary Proceedings

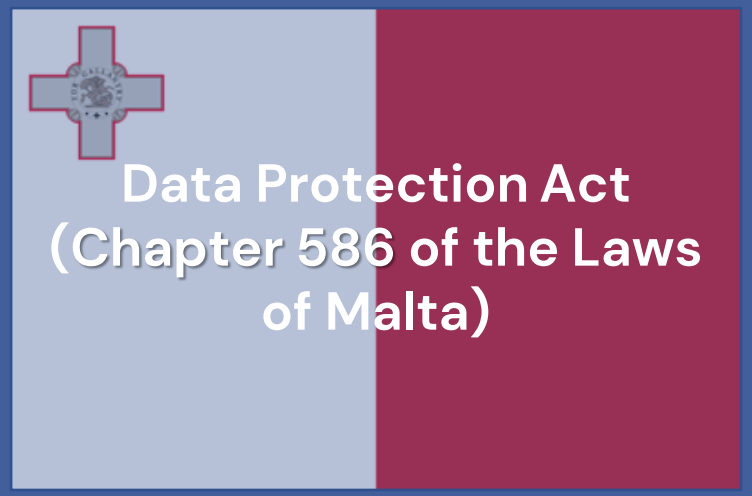
- Same rules should apply as under normal proceedings – decide on whether physical meeting will be adopted or whether online meetings are also an option;
- Means used – technology works properly and is appropriate for the purpose used; employee is still given access to any documents.
- Ensure confidentiality – anyone concerned should be alone in the room & inform about any recording taking place.
- Give access to documents and inform about any witnesses.
- Still allow individual to be accompanied.

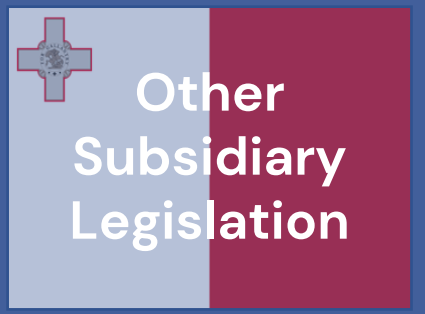
MAMO TCV
ADVOCATES

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

www.gdprmalta.com

MAMO TCV
ADVOCATES





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

The GDPR came into effect on 25 May 2018

MAMO TCV
ADVOCATES

www.gdprmalta.com

www.21Academy.education

Non-Applicability of the GDPR

Processing undertaken by an individual in the course of a *purely* personal or 'household' activity (see Rynes CJEU case)

Processing for purposes of public/national security, defence, State security etc.

Files or sets of files not structured according to specific criteria

Processing of anonymous data

Processing of personal data of deceased individuals

Criminal law (different laws Apply)

Territorial Scope of the GDPR:

- An organization (controller **or processor**) '*established*' in the EU is subject to the GDPR.

- An organization (controller **or processor**) based *outside* the EU is subject to the GDPR if it either:

  - **A) '*offers*' goods or services to data subjects in the EU; or**
  - **B) '*monitors*' the behavior of data subjects in the EU.**

MAMO TCV
ADVOCATES

Transfers of Data Abroad

Transfer to a 'third country' (i.e. Non-EU/EEA) of personal data that is undergoing processing or intended processing, may only take place subject to the provisions of the GDPR or other *ad hoc* arrangements

- The 'third country' to which the data is transferred must ensure **an adequate level of protection.** This includes when employees are working remotely outside the EU and accessing personal data.
- Transfers to countries <u>not</u> offering such adequate level of protection may still take place without needing IDPC approval if '**appropriate safeguards**' are in place.
- These 'safeguards' include **EU Model Clauses**, **Binding Corporate Rules** (which will still require IDPC approval), an approved **Code of Conduct** and an approved **Certification Mechanism.**
- **UK** is whitelisted.
- **USA** remains an issue.
- In absence of the above grounds, other grounds may still justify the transfer (for example, the **explicit consent of the data subject**).

FAMILIARISE YOURSELF WITH KEY TERMINOLOGY

PERSONAL DATA & SENSITIVE PERSONAL DATA

DATA CONTROLLER

PROCESSING

DATA PROCESSOR

DATA SUBJECT

DATA PROTECTION OFFICER

Mamo TCV Advocates

PERSONAL DATA (AND DATA SUBJECTS)

Definitions of Key Terms

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject').

An identifiable natural person is one who can be identified, directly or indirectly, *in particular* by reference to an **identifier** *such as*:

- A name;
- An identification number;
- Location data;
- An online identifier (IP address, Cookies, device IDs etc.);
- One or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

NB 1 the GDPR does not apply to the processing of **anonymous data**.

NB 2 the GDPR does not apply to the processing of **personal data of deceased persons.**

Are the following ‘personal data’?

- Car licence plate — Yes
- Job Title — No — But if there is only one (well-known) person with that job title, Yes
- Tattoo — Yes
- Blood — With the right tools, Yes
- Mr Arthur and Mrs Claire Galea have inherited Mr Andrew Mifsud.

Pseudonymisation

Definitions of Key Terms

- **'Pseudonymisation'** *means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

MAMO TCV ADVOCATES

Pseudonymisation

Definitions of Key Terms

- **'Pseudonymisation'** *EX*:

List A	*List B*
• *Employee A*	• *Brad Pitt*
• *Employee B*	• *Leonardo da Vinci*
• *Employee C*	• *Cristiano Ronaldo*
• *Employee D*	• *Warren Ciantar*
• *Employee E*	• *Freddie Portelli*

MAMO TCV ADVOCATES

Special Categories of Personal Data (Art. 9)

(Formerly 'sensitive personal data')

Definitions of Key Terms

Means Personal Data that reveal:

- Race or ethnic origin, or
- Political opinions; or
- Religious or philosophical beliefs; or
- Trade union membership; or
- Data concerning health or
- Data concerning a natural person's sex life or sexual orientation.

As well as Processing of:

- Genetic data (genes, gene products etc.)
- Biometric data (fingerprints, retina and iris patterns etc.)

Stricter rules apply to the processing of **sensitive** personal data

MAMO TCV ADVOCATES

Criminal Conviction Data

- Under the GDPR and the Maltese DPA, **data relating to offences or criminal convictions** may only be processed **under the control of a public authority** and **under strict requirements**, except as may be authorised by regulations and subject to suitable safeguards in accordance with Article 10 of the GDPR.

- The GDPR also specifically states that a complete register of criminal convictions can only be kept by a public authority.

- There are presently no Maltese derogations to this general rule.

MAMO TCV
ADVOCATES

21 ACADEMY

What About ID Cards?

Under the DPA, ID Cards may only be processed (i.e. including storing of such information):

1) **With the data subject's consent**

2) **In the absence of consent if the processing is clearly justified by:**

   A) **The purpose of the processing;**

   B) **The importance of a secure identification;**

   C) **Another valid reason prescribed in regulations.**

IDPC: "*Copies of ID cards can only be stored in exceptional cases where a law specifically requires or authorises such processing*" (e.g. AML laws).

MAMO TCV
ADVOCATES

PROCESSING

Definitions of Key Terms

*Any operation or set of operations which is performed on personal data or on sets of personal data, **whether or not by automated means**, such as:*

- *collection,*
- *recording,*
- *organisation,*
- *structuring,*
- *storage,*
- *adaptation*
- *alteration,*
- *retrieval,*
- ***use,***
- *consultation,*
- *disclosure by transmission,*
- *dissemination or otherwise making available, alignment or combination, restriction,*
- *erasure or destruction.*

'Processing' covers almost any possible use of pe data

MAMO TCV ADVOCATES

DATA CONTROLLERS

Definitions of Key Terms

A "**Controller**" of personal data is the **natural or legal person**, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**;

MAMO TCV
ADVOCATES

DATA PROCESSORS

Definitions of Key Terms

- A *"Processor"* is a natural or legal person, public authority, agency or other body which processes personal data **on behalf of** the controller;

  Ex: Outsourced service providers (IT providers, Web administrators, HR services, Payroll services etc.)

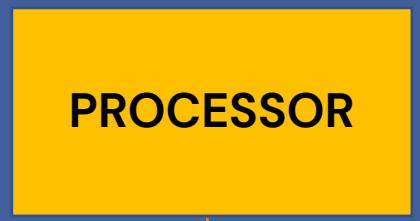
- The relationship between the Controller and Processor must be **contractual** in nature.

ONLY WHERE PERSONAL DATA ARE PROCESSED

- 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)

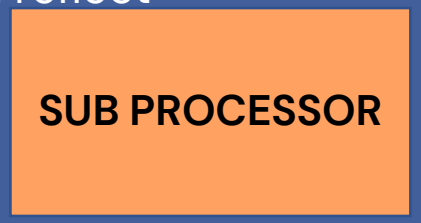
DPA must be in place here



- **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**)
- IT Service Provider
- Security Service Provider

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



- **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**)

- **Joint Controllership** (Art. 26,GDPR)

- **Separate Controllership**: (No GDPR clauses)

Other Scenarios:

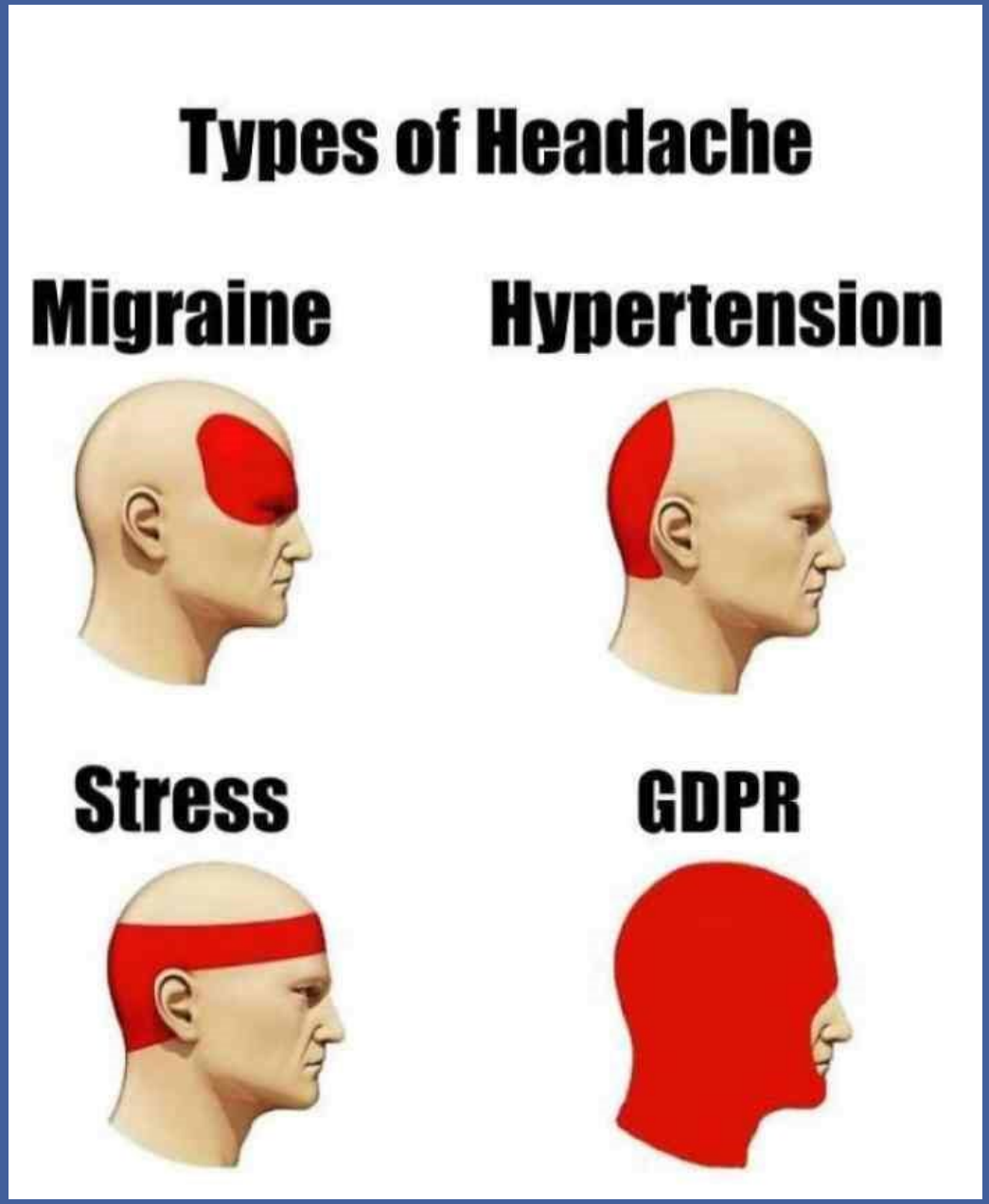
- Where no personal data are shared between the Controllers.

- Where personal data are shared between the Controllers (ex. referral arrangements).

MAMO TCV
ADVOCATES

Art 28(3) - Data Controller – Data Processor Contract must stipulate in particular that the processor:

(a) processes the personal data only **on documented instructions** from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
(b) ensures that persons authorised to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality;
(c) takes all measures required pursuant to **Article 32**;
(d) respects the conditions referred to in paragraphs 2 and 4 for **engaging another processor**;
(e) taking into account the nature of the processing, **assists the controller** by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assists the controller in ensuring compliance with the obligations pursuant to **Articles 32 to 36** taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, **deletes or returns all the personal data to the controller** after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
(h) makes available to the controller **all information necessary to demonstrate compliance** with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.



MAMO TCV
ADVOCATES

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**

MAMO TCV
ADVOCATES

21 ACADEMY
www.21Academy.education

Lawfulness, Fairness & Transparency

Controllers must ensure that data subjects are not misled as to the **purpose of the processing.**

Data subject must be told what processing will occur (**transparency**), the processing must match this description (**fairness**) and the processing must be for one of the purposes specified at law (**lawfulness**).

Data subjects must also be informed of any other organisations that will use the information and the purpose of such use.

MAMO TCV
ADVOCATES

- The ‘Data Quality Principles’ must <u>always</u> 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 ***<u>lawful</u>*** to process this personal data at all?”

“If so, on what ground(s)?”

MAMO TCV
ADVOCATES

Lawful Grounds for Processing Personal Data under the GDPR:

(Art.6, GDPR)

- Consent
- Contractual Necessity
- Legal Obligations
- Vital Interests
- Public Interest/Official Authority
- Legitimate Interests

MAMO TCV ADVOCATES

MAMO TCV ADVOCATES

Identifying the Correct Legal Basis

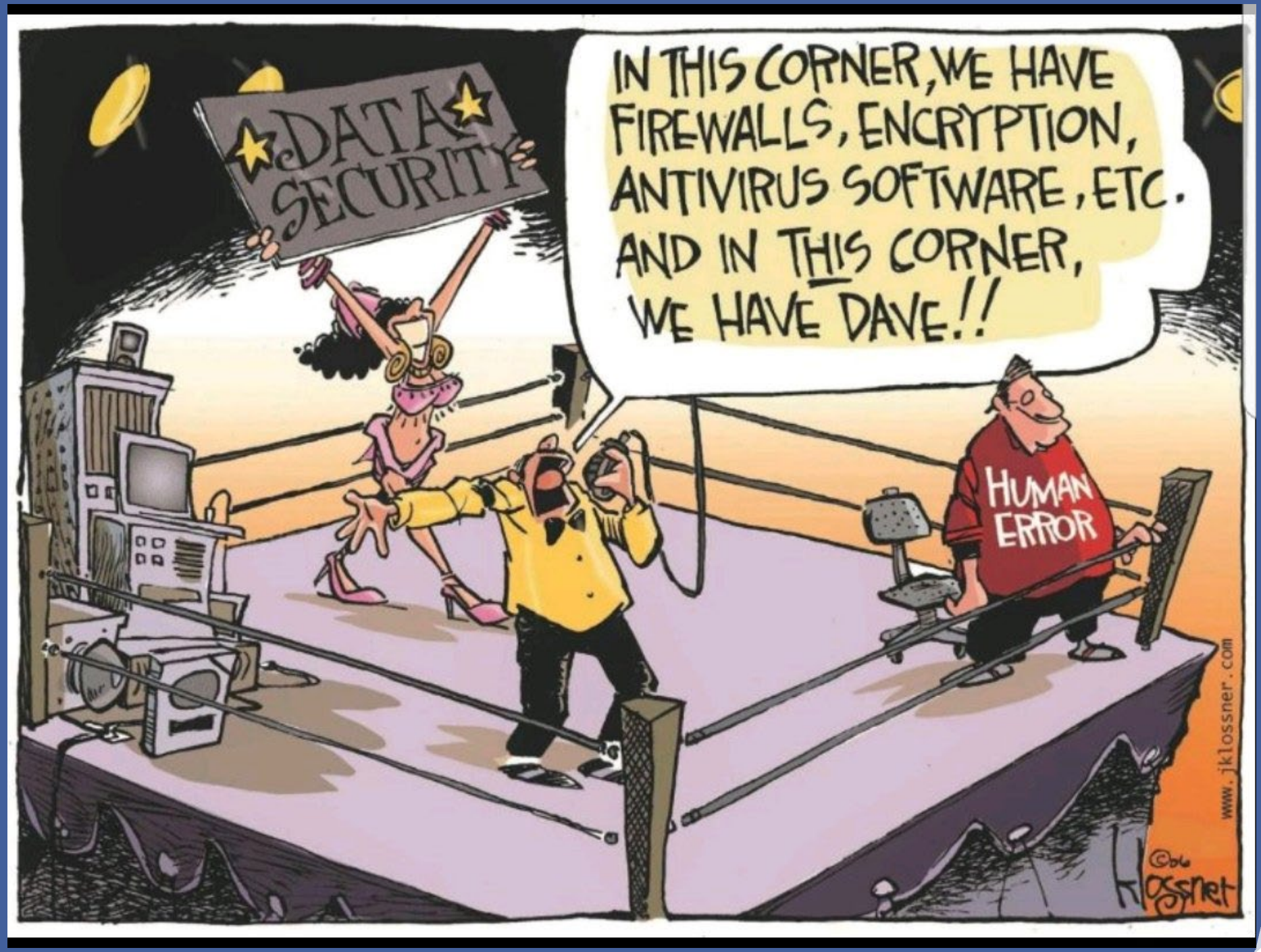
Q. What legal basis should an **employer** use to process personal data of **employees**?

Necessity for the compliance of Contractual Obligations and Legal Obligations. This allows for the most convenient method of processing. The employer must simply inform the employee of the legal basis (bases) being used.

Consent is a very bad choice for many reasons: differing positions of power; consent cannot be said to have been freely given; what happens if it is withdrawn?

(VIP) - Security Measures

- Controller (and Processor) is obliged to implement **appropriate technical and organisational measures** to protect the personal data that is processed against accidental destruction or loss or unlawful forms of processing;
- Thereby providing an **adequate level of security**, due account being taken of relevant factors (sensitivity of data, cost, technical means, risks);
- GDPR mentions **encryption**, on-going reviews of security measures, redundancy and back-up facilities, regular security testing etc.);
- Strongly recommended: **2-factor authentication** and having **complex passwords (10+ characters, including lower/uppercase, numbers and symbols)** (https://www.security.org/how-secure-is-my-password/), among various other more complicated IT measures;
- Have policies in place that employees must adhere to or are informed of: **IT/security policy, BYOD policy outboarding policy** etc. – Can all be presented in the form of a handbook.
- Even more important now that employees may be working in a less secure environment at home.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©bu
Klossner

Data Breach Notification (IDPC) – Art. 33

The GDPR introduces a **new obligation**

Definition of a Personal Data Breach:

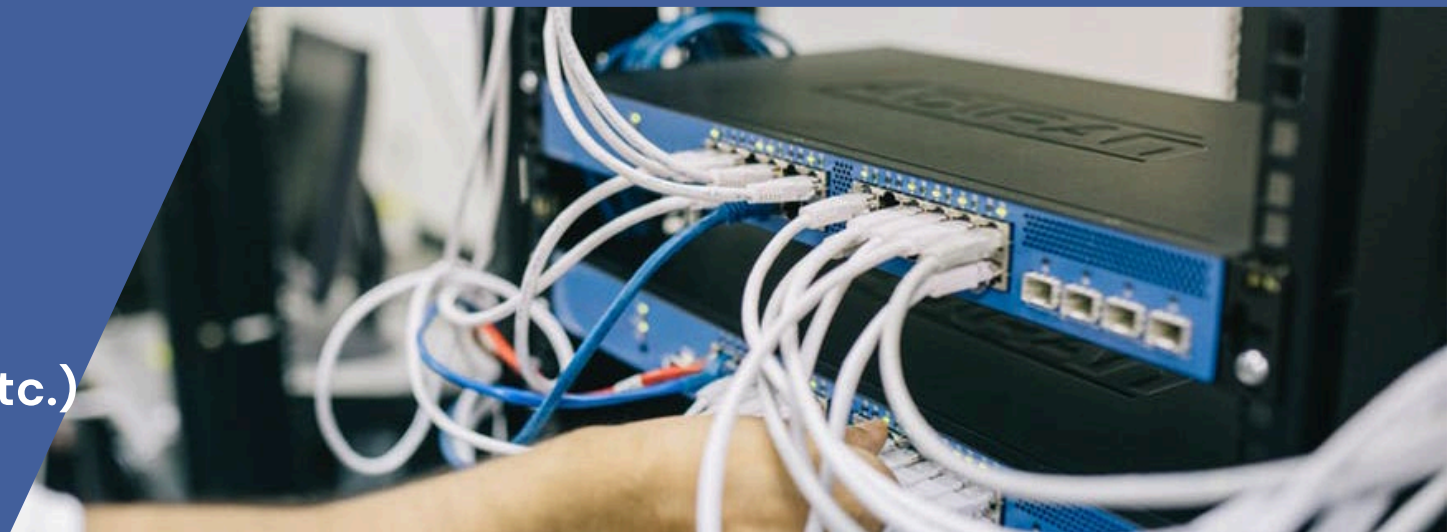
A breach of security leading to the accidental or unlawful:

- **Unauthorised access to processed personal data;**

or the

- **Destruction,**
- **Loss,**
- **Alteration, or**
- **Unauthorised disclosure,**

of personal data being processed (stored etc.)



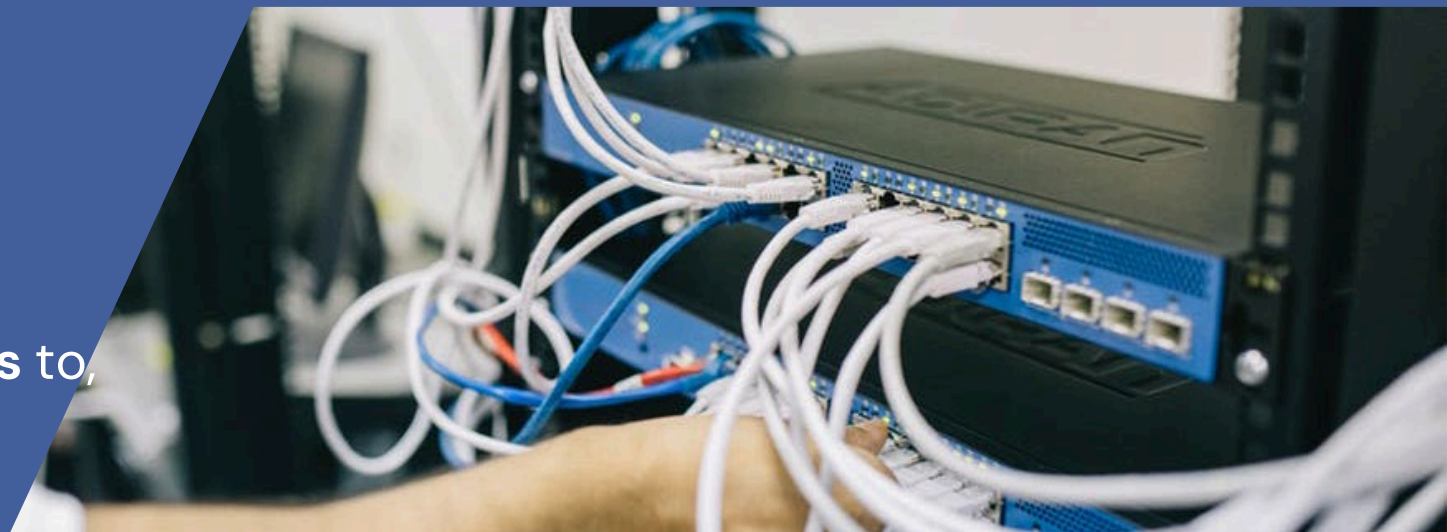
Data Breach Notification (IDPC) – Art. 33

The GDPR introduces a **new obligation**

Definition of a Personal Data Breach:

The WP 29/EDPB Guidelines categorise breaches into 3 categories:

- "Confidentiality breach" – where there is an unauthorised or accidental **disclosure** of, or access to, personal data.
- "Integrity breach" – where there is an unauthorised or accidental **alteration** of personal data.
- "Availability breach" – where there is an accidental or unauthorised **loss of access** to, or destruction of, personal data.



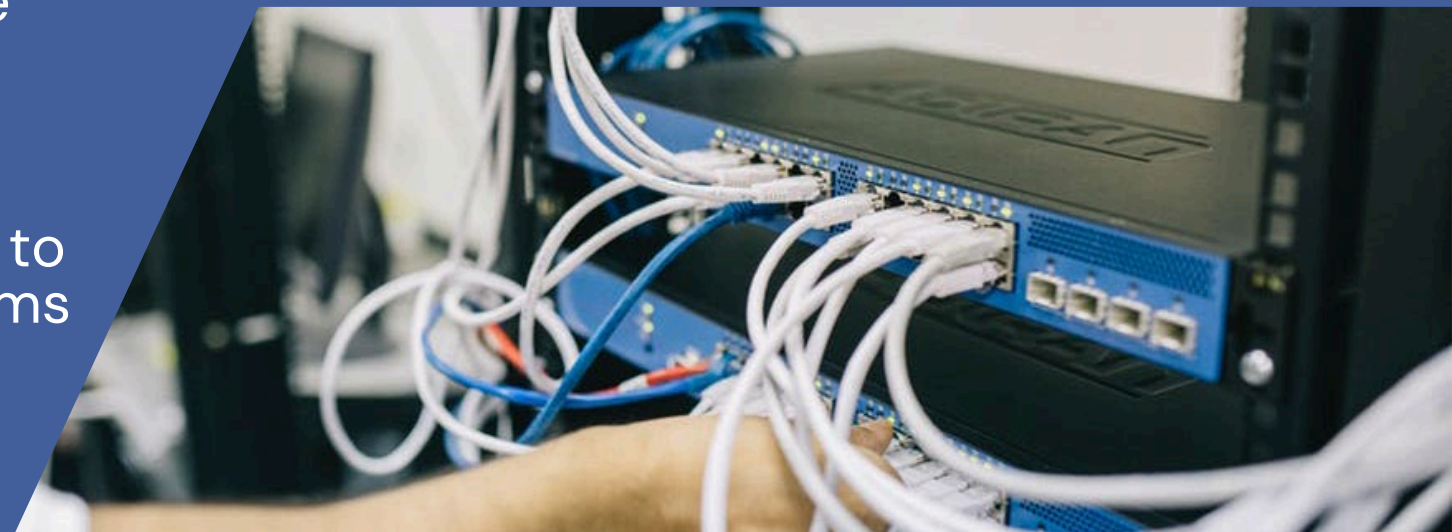
Data Breach Notification (IDPC) – Art. 33

The GDPR introduces a **new obligation**

General Rule: In the event of a data breach, the Controller must report the breach to the IDPC without undue delay and in any event, **within 72 hours** of becoming aware of it.

NB – Processors must notify such breaches to Controllers '*without undue delay*'. The Controller's deadline commences upon being notified by the Processor.

Exception: breach notification is **NOT** required where data breach is ***unlikely*** to result in any ***risk*** to the rights & freedoms of data subjects.



Data Breach Notification (IDPC) – Art. 33

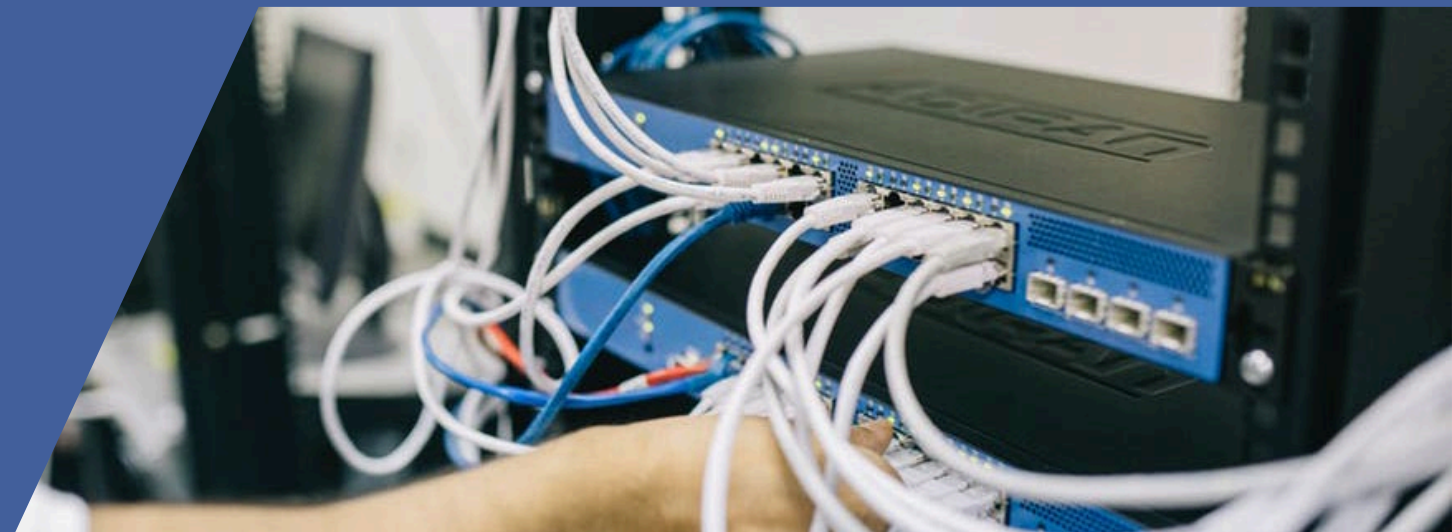
The GDPR introduces a **new obligation**

Notification Must include:

- Description and nature of breach,
- Approximate number of affected data subjects,
- Categories of data and approximate number of records affected,
- Name and contact of the DPO or other contact point,
- Likely consequences of the breach,
- Measures taken by Controller to remedy/mitigate the breach.

In any case, **all breaches must be recorded** no matter how big or small and reported to the IDPC on demand.

Internal procedures must be implemented ASAP to comply with this new obligation.



Data Breach Notification (Data Subjects) – Art. 34

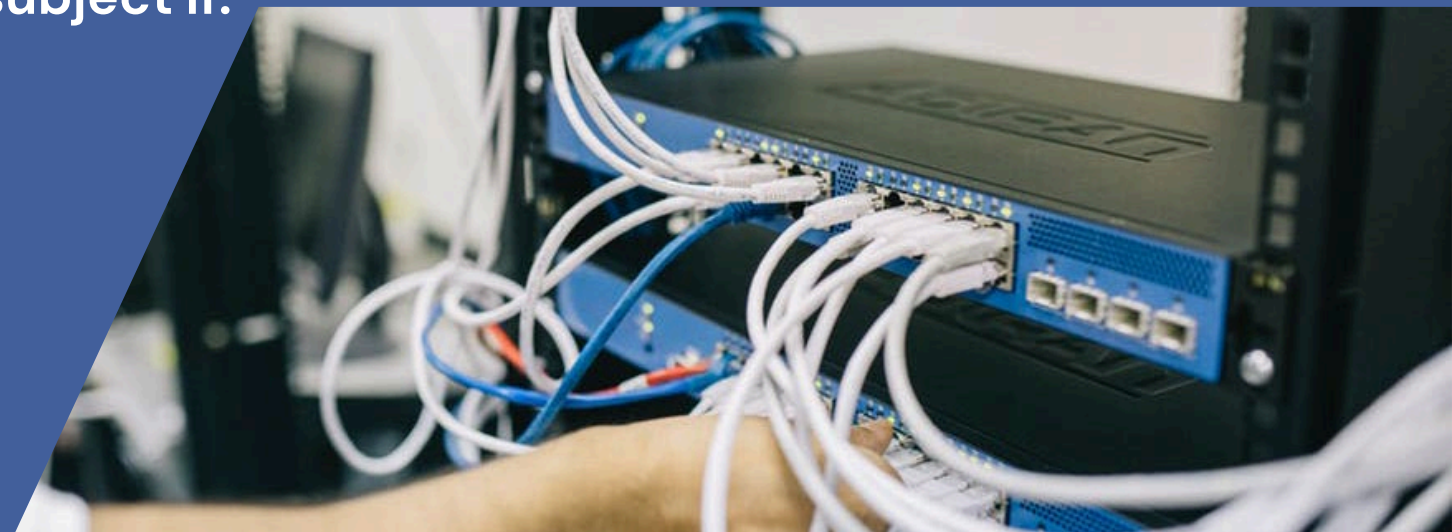
The GDPR introduces another similar **obligation**

In the event of a data breach causing a '***high risk***' to the rights and freedoms of data subjects, the Controller must notify the *affected data subjects* without undue delay;

Notification to include: The **nature of the breach**, the **name and contact of the DPO** or other contact point, the likely **consequences** of the breach and the **measures taken** by Controller to remedy/mitigate the breach.

Controller is exempt from notifying data subject if:

- **Risk of harm is remote because data is protected** (ex: with strong encryption)
- **Controller has taken measures to protect against the harm** (suspending accounts etc.)
- **Notification would require disproportionate efforts** (public notice must be issued here).



Identifying a Data Breach

Q. If I have lost a password-protected pen drive containing a copy of highly sensitive personal data about ALL my clients, is that a data breach?

No, because whoever finds it has no way of accessing the data and I've only lost a copy, I still have the original data.

Data Breach Notification (Some Tips)

1) Before sending out personal data (especially via email) MAKE SURE IT IS THE CORRECT RECIPIENT. Watch out for cc and bcc lines;
2) Carry out an IT audit to check security obligations (to prevent data breaches in the first place);
3) Train your employees;
4) If you suspect that a data breach has occurred, speak to your DPO (or other responsible person) and your legal counsel immediately.

NB - Remember the 72 hours deadline

Data Breaches – Likely or Not?

- Q4 2020 currently holds the record for number of online data breaches experienced by Internet users at 125.75 million
- Cybercriminals can penetrate 93% of company networks, especially now in a post-pandemic world where so many employees work from home
- In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year
- The majority of data breaches (around 80%-90%) are caused by human error rather than cyber-attacks
- The most common causes of cyber-attacks are malware and phishing
- In Malta, up until end of 2021, 424 data breaches were reported to the IDPC - 83 of them last year alone (nearly 20%)
- To date, the IDPC has issued 37 fines (some are being appealed in Court)
- Unfortunately, it is a question of "*when*" rather than "*if*"

MAMO TCV ADVOCATES

21 ACADEMY

www.21Academy.education

What if I don't Notify when I should have?

- October 2022 - Zoetop (parent company of fast-fashion site Shein) fined **€1.95 *million*** for its poor handling and reporting of a data breach. 39 million Shein accounts' login details were stolen and Shein tried to downplay it by reporting that only 6.42 million accounts had been exposed.
- May 2019 [Lithuania] – Payment Service Provider fined **€61,500 –** The supervisory authority was carrying out an inspection and noted that the controller was processing more personal data than necessary. Also, during a 24 hour period in July 2018, payment data was publicly available on the internet due to inadequate technical and organisational measures, affecting 9,000 payments with 12 banks across the globe.
- April 2019 [Hungary] – Undisclosed political party fined **€34,375** – Cyber attack by anonymous hacker who accessed and disclosed information on how vulnerable the party's system was, compromising a database of over 6,000 individuals. The hacker published the command one could run to carry out the attack, so even people with very little IT skills could access the information from the database.

In the above cases, the supervisory authority came to the conclusion that the entity should have submitted a data breach notification, but the controller didn't OR that the controller was not entirely honest when reporting or even lied about the facts or failed to notify the data subjects when it should have.

Monitoring During Employment

- Development of potentially more intrusive means of monitoring – not only monitoring of email or website use;
- Monitoring all online activity of employees – disproportionate interference with data subjects' rights.
- Importance of written policies re monitoring – allows employees to adapt their behaviour.
- Consider – proportionality + acceptable use policies.

Monitoring at the Workplace

- Necessity to protect network and preventing unauthorised access or data leakage – employer might implement measures to monitor online activity of employees;
- Good practice:
- provide alternative unmonitored access for employees ex. Free WiFi for private usage;
- No interception of certain kind of traffic ex online banking and health websites;
- Clear policy about acceptable and unacceptable use of the network and facilities;
- If possible block certain websites as opposed to monitoring use.

Monitoring ICT use Outside the Workplace:

- Remote working – may result in breaches to employer's security/ loss of information etc – what means are permissible to monitor activity?
- Bring Your Own Device (BYOD) – can lead to employers processing non-business related information;
- Mobile Device Management (MDM) – enables employers to locate devices remotely and even delete date on demand.
- Tracking of vehicles used by employees for work purposes – duty to inform and switch off tracking after working hours.

Monitoring Cont:

Ownership of an electronic device does not necessarily mean that the employees do not enjoy the right to secrecy of their communications, related location data and correspondence.

Prohibiting all communications for personal reasons is not practical & might require a high level of monitoring which is disproportionate.

On-Premises Monitoring

CCTV - General rules:

- 7-day retention period for footage (extendable to 20 days in limited cases with IDPC approval)
- Camera must not be pointed at areas you do not own/control
- Sound recording should be avoided wherever possible
- Cameras should not be pointed directly at employees' terminals/workstation
- You can (and in most cases *must*) provide footage to the police if they ask for it (provided you still have it – if you don't, it's not an infringement at your end)
- Ensure that any security contractors also abide by data protection law (have a DPA in place if they process personal data on your behalf)
- Individuals under surveillance may exercise their right of access
- **No covert recording** - You must always notify data subjects via a notice as per EDPB template

MAMO TCV
ADVOCATES

CCTV Notice – EDPB Template

(Note the legal basis being used)

	Identity of the controller and where applicable, of the controller's representative:
	Contact details of the Data Protection Officer (where applicable):
	Purposes of the processing for which the personal data are intended as well as the legal basis for the processing: Our legitimate interests to ensure adequate security on our premises, for crime-prevention purposes [and for monitoring of work-related activity].
Further information is available: • Via the notice provided to you • At our reception/customer information/HR manager • On our website (URL/QR Code: ___)	**Data subject rights**: As a data subject you have several rights against the controller, in particular the right to request from the controller access to or erasure of your personal data. For details on this video surveillance including your rights, see the full information provided by the controller through the options presented on the left.

MAMO TCV ADVOCATES

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.

IT/Remote Monitoring

- Examples include:

Keyloggers, Screen capture devices (either constant or timed), Activity/Email tracking, Trackers in vehicles, time tracking, website blockers

- Some are more intrusive than others

- Useful to ensure employees are productive and accountable, can also help with billing and accounting

- Allows more flexibility in whom to hire, as employer can be confident of the employee's productivity even if they are working remotely

- **No covert monitoring** - You must notify data subjects of any monitoring tools installed on their device(s) – can be done via employee handbook or an *ad hoc* policy/notice circulated internally

MAMO TCV
ADVOCATES

The GDPR came into effect on 25 May 2018 – What's happened since then?

MAMO TCV
ADVOCATES

21 ACADEMY

www.21Academy.education

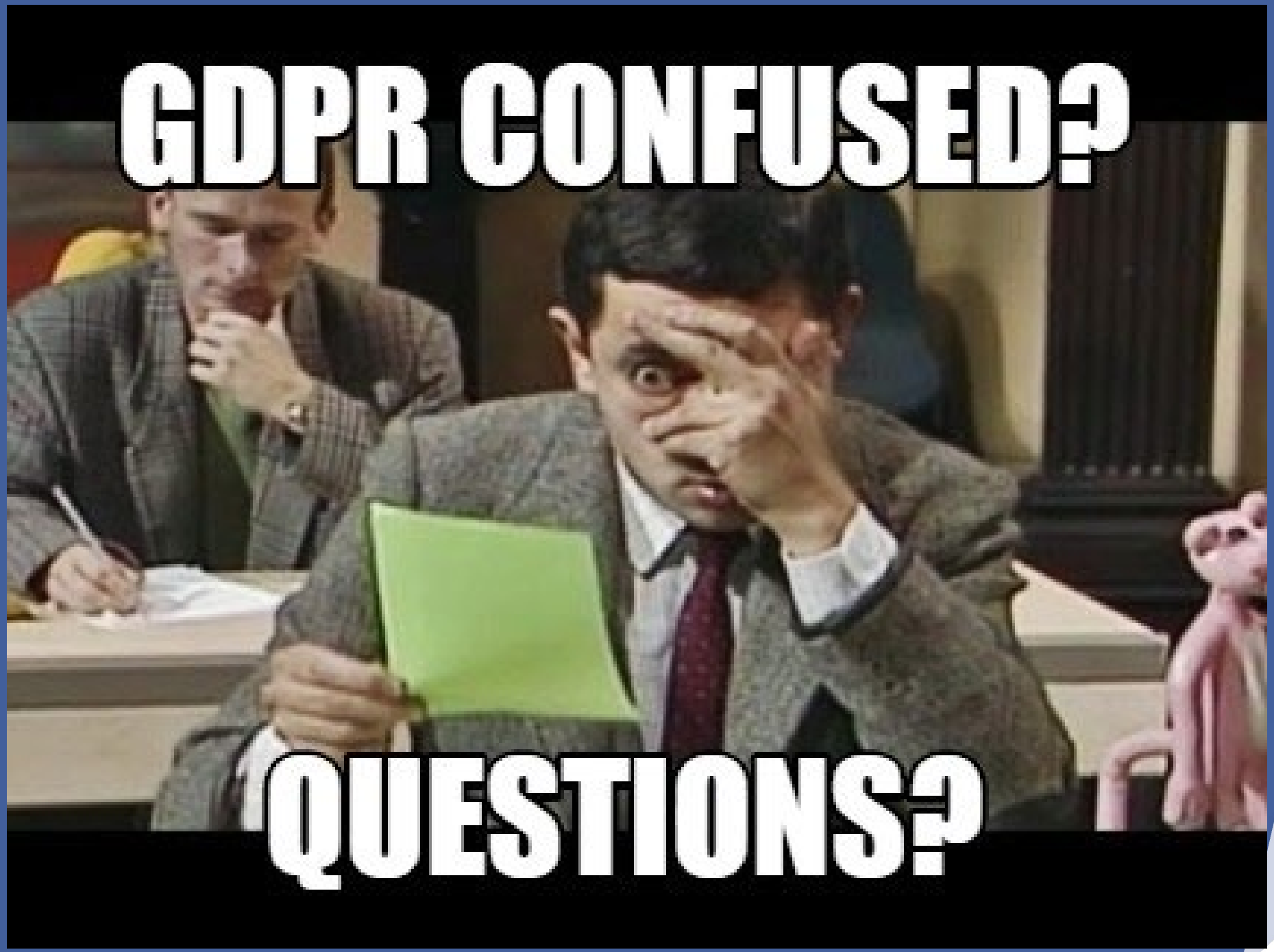
Some Practical Tips

- In the majority of instances, problems will arise from 3 sources:
    1. Disgruntled employees
    2. Disgruntled clients
    3. Competitors
- Carry out regular training for staff, if necessary, grouping it with training on other matters. GDPR compliance is not a one-time thing, it must be an ongoing practice – remember that: people forget and new employees will join who may have never received such training.
- Employees should be able to flag any suspicious activity, be it a data breach, security incident etc. and report it immediately.
- Wherever possible, and depending on the size of your organisation, do not leave GDPR compliance up to one person – the topic is vast and can be overwhelming for one individual.
- Ensure that you actually *implement* any policies you have. Putting up a privacy policy on your website is the easy part.

Benefits of GDPR

- It has had a profound impact on not just the EU, but the entire world.
- It has set a high bar for other non-EU countries to reach, prompting many countries to revamp their own privacy regimes.
- Some have gone as far as to say that the biggest impact of GDPR has been felt *beyond* Europe.
- Politicians and technology CEOs now include privacy among their topics of discussion, because of GDPR. Privacy has become a worldwide concern, as it should be.
- Privacy by design and default has become more mainstream and given rise to "ethics by design" and "security by design". Having software created with such issues in mind from the get-go, not retro-fitting later on.
- It merely formalised what should have always been there: trust, respect and a customer-centric attitude in all organisation structures.

MAMO TCV
ADVOCATES


GDPR CONFUSED?
QUESTIONS?

Thank you for your attention!