Legal and Professional Issues

Theme 5 Notes

Part A

GDPR – General Data Protection Regulation

- **PRIVACY: BEFORE GDPR**

Emergence of Privacy:

'The right to privacy' – Harvard Law Review of 1890

Warren and Brandeis complained that:

"The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle."

Central thrust of the article - Common law should protect 'privacy':

Referred to Mr Justice Cooley

'Right to be left alone' – 2 years earlier

" The common law has always recognised a man's house as his castle, impregnable, often even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?"

Ireland

Limited recognition of privacy in the Constitution:

"State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen." – Art 40.3

"State pledges itself to guard with special care the institution of Marriage, on which the Family is founded, and to protect it against attack." – Art 41.3.1

"The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with the law." – Art. 40.5

Other Legislation & Cases further define privacy:

- Data Protection Acts 1988-2003 (now superseded)
- Limits on Privacy (Common Good)
- Haughey v. Moriarty 1999
- Bailey v. Flood 2000
- DPP v. McCann 1998 (Privacy v. Right to Life)
- National Irish Banks v. RTE 1998 (Freed. Of Express)

McGee v. Attorney General 1974 (Marital Privacy)

Supreme Court Held:

"… it is scarcely to be doubted in our society that the right to privacy is universally recognised and accepted with possibly the rarest of exceptions, and the matter of marital privacy must rank as one as one of the most important matters in the realm of privacy."

Kennedy & Arnold v. Ireland 1987 (Comms Privacy)

Phone Tapping: s56 Post Office Act 1908

Warrant should only be issued:

- State security & serious crime prevention
- State maintained that it acted legally and did not interfere with constitutional rights

Although privacy was "… not specifically guaranteed by the Constitution, the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the state."

An Unenumerated Right:

- *"right to privacy includes… respect of phone conversation…"*

Not an absolute right

If so: many functions of state would cease

E.g. No taxes could be collected

Haughey v. Moriarty 1999

"there is no doubt but that the plaintiffs enjoy a constitutional right to privacy. What is in dispute… is the extent of such a right… whether it extends to the right of banking transactions and whether the exigencies of the common good outweigh."

Redmond v. Flood 1999

A challenge to certain investigations by Flood

"Common good require that matters considered by… Oireactas to be of urgent public importance be inquired into…"

Bailey v. Flood 2000

SC refused leave for a Judicial review of Def. actions

However in **Norris v. AG 1984**

- SC refused to recognise absolute individual privacy
- Privacy yields to right to maintain public morals
- Later: State changed its mind (ECtHR)
- Enacted Criminal Justice (Sexual Offences) Act 1993

DPP v. McCann 1998

Right to privacy inferior to right to life

Garda sought adoption papers

"… obligation on the State to discover why such fundamental constitutional rights has been unjustly extinguished…"

NIB v. RTE 1998

- Privacy balance against Freedom of Expression
- Public interest in defeating wrongdoing
- Public interest out weights confidentiality

Different people, different rights

- **Ahearne & Ahearne v. RTE 2005**
- Leas Cross nursing home
- 3 categories: nurses, patients & owners
- **Von Hannover v. Germany 2004 – EctHR**

Waiver of the right to privacy

- **McGrory v. ESB 2003**
- Plaintiff sued ESB for personal injuries
- ESB entitled to enquire into his medical conditions

Privacy as Property

- **Douglas v. Hello 2005**
- Sold rights to wedding photos
- Right to confidential information not right to privacy
- **Jane O'Keefe v. RyanAir 2002**
- Compromise privacy for compensation

Privacy v. Freedom of Expression

The rights of privacy and freedom of expression are both fundamental.

In media cases they are often in direct conflict.

The theoretical problem of the "balancing of rights" is a pressing practical issue for editors as well as media lawyers.

Campbell v. Mirror Group Newspapers (2004 UKHL 22)

First opportunity post UK Human Rights Act 1998.

Daily Mirror discovered that, despite her public denial of drug use, Ms Campbell was secretly attending meetings of Narcotics Anonymous and published an article and an photo.

Court analysed the article

Five elements of private material:

- the fact of Ms Campbell's drug addiction
- the fact that she was receiving treatment for addiction
- the fact that she was receiving treatment at Narcotics Anonymous
- details of that treatment and her reaction to it
- surreptitiously obtained photographs of her emerging from a treatment session

Two fundamental issues arose:

- Extend of unjustified publication of private information protection?
- How to reconciled with the right to freedom of expression?

Private Information

In relation to the first issue, the Court recognised that breach of confidence should be expanded so as to provide a remedy for the unjustified publication of personal information.

Held: the Human Rights Act 1998 now meant the law of confidence has absorbed the values protected by Article 8 (privacy) and Article 10 (expression).

Private protection should be determined by applying an objective test of "reasonable expectation of privacy".

Lord Hoffmann:

"a photograph of humiliation o severe embarrassment may infringe."

Balancing Rights:

Held that Article 8 and 10 rights should be balanced by applying the principles of proportionality.

Neither right takes precedence over the other.

It was recognised both that some types of speech are of greater value than others and that there are difference degrees of privacy.

3-2 Decision in Campbell's flavour:

- details of therapeutic treatment for addiction was private
- disclosure could interfere with or disrupt her treatment

Campbell's Legacy

Does not prevent publication about the private lives of politicians or celebs.

Does require a more rigorous approach to deciding publication.

Suggested approach:

- consider whether publication contains material which has a reasonable expectation of privacy.
- If so, consider whether a "public interest" defence exists for this.
- If such a defence does not apply to each element, then necessary to consider how private the information is and what type of speech is involved.
- If information is intimate, publication must have some political and democratic value to justify its publication.
- Photographs should be considered separately where they depict humiliating or embarrassing events or have been obtained surreptitiously, then publication will be difficult to justify.

➢ GENESIS

Conception of DP is a very modern

- Digitally stored databases and records:
    - Digital records are intangible, no physical weight, and can be lost or stolen without indication. Such a loss could represent an enormous amount of value.
- Earliest information protection were driven by the professions rather than law:
    - e.g. Lawyer-client privilege became a sort of contract between a lawyer and client over the centuries.
        - ❖ Allowing the lawyer to represent their clients' interests without the client fearing legal repercussions.
    - e.g. Medical records and a doctor's confidentiality were established. Though a court could force those records to be handed over, the medical profession otherwise kept them relatively safe.
    - These practices ensured specific silos of personal information were protected according to the interests of the business. Where a business value existed then information was protected.
- Moving from paper to electronics meant more varied & powerful methods for manipulating personal information. This means greater risks.
    - e.g. Political campaigns have used increasing volumes of data to better target key demographics, define policy, manage candidates' image, etc.
        - ❖ Campaigns targeted states based on historical notions of which states were "swing" i.e. could go either way and budget realities.
        - ❖ Campaigns also use data to construct predictive models to make targeting campaign communications more efficient and to support broader campaign strategies. These predictive models result in three categories of "predictive scores" for each citizen in the voter database: behaviour scores, support scores and responsiveness scores.
    - e.g. Identity theft has become a significant problem that has only become a greater threat with the greater volume of information that is available.

Europe

European Convention on Human Rights (ECHR) in 1953 – Article 8

'Everyone has the right to respect for his private and family life, his home and his correspondence.'

'There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, …'

Council of Europe – 1981

- Treaty 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Established standards to ensure the free flow of information throughout EU member countries without infringing personal privacy.
- 1988 – Data Protection Act
    - Reflected the minimum standards specified in the convention.
    - Not rigorous in 1988. Requirements for the protection of personal data were considerably less urgent than today.
    - The power and availability of computers exploded during the 80s and 90s.
    - EU Member States' data protection laws diverged, thus impeding data flows through the EU and thus impeding business.

Data Protection Directive – 1995

- Reset for DP, obligating all member states to align with it and thereby improve protections for personal data, while simultaneously reducing the burdens impeding the free flow of data through the Union.

- Established rules for transporting data outside of the EU. e.g. US-EU Safe Harbour framework.
    - Which asserted that US data protection laws were sufficient for the protection of personal data originating in the EU, as long as the recipient in the US observed a set of data protection principles.
    - Found to be in breach of the DPD in 2015, it did support considerable business activity for 15 years (Schreme Case)

- Data Protection Act 2003
    - Enacted the requirements of the DPD
    - Founded on 8 principles:
        1. Obtain and process information fairly.
        2. The data must be kept for a specified lawful purpose.
        3. The data should be used and disclosed only for the specified purpose.
        4. The data must be kept safe and secure.
        5. The data must be up to date, accurate and complete.

6. The data must be relevant, adequate but not excessive.
7. The data must be retained for no longer than is necessary.
8. A copy of the data must be made available to the data subject, on request.

These principles clearly laid out the general aims of the Ac, which made it reasonably simple to determine whether an organisation was meeting its obligations. There was some complexity in the broader Act, however, and repeated amendments and updates meant that it continued to grow and become more unwieldy as time went one.

- Mis-alignment: Across the EU, other, similar legislation was enacted, but through a combination of time and varying national interests, no two national interests, no two national laws were sufficiently similar for an organisation to simultaneously be compliant in its home country and across all the other EU member states.

  That is, the free flow of information was effectively inhibited because the different regulatory environments clashed on matters of detail, requiring businesses and governments alike to arrange processes specific to an increasing array of scenarios.

- General Data Protection Regulation (GDPR) – 2018
  - Regulation: a law and enters into force across the Union simultaneously. Not dependent on the interpretation of the local government, courts or authorities. Because of the legal weight of a regulation, they typically take much linger to pass through the legislative process, but they also ensure greater consistency across the Union.

➢ **DEFINITIONS**

- Data Controller (DC): 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.
- Data Processor (DP): Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- Data Subject (DS): "An identified or identifiable natural person." There is no restriction on their nationality or place of residence, so a data subject can be from anywhere in the world. Equally, however, a data subject has to be a person. A corporation or other entity cannot be a data subject, and information on those subjects has no protection under the Regulation.
- Personal Data: Means any information relating to an identified or identifiable natural person is one who can be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- Biometric Data: Data processing relating to the physical, physiological or behavioural characteristics of a person, which confirm the unique identification of that natural person, such as facial images or finger print data.
- Genetic Data: Data relating to the inherited or acquired genetic characteristics of a person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- Consent: 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.
- Binding Corporate Rules (BCRs): Policies which are adhered to by organisations established in the EU for transfers of personal data within a group of undertakings engaged in a joint economic activity.
- Cross-Border Processing: Processing by the activities of establishments in more than one Member State of DCs/DPs in the EU. OR processing of personal data by a single DC/DP in EU but which substantially affects DSs in more than one Member State.
- Data Concerning Health: Data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status.
- Filing System: Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- Main Establishment: As regards a DC with establishments in more than one Member State, the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment. As regards a DP with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.
- Data Breach: Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- Processing: This means 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 or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- Profiling: Automated processing of data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- Pseudonymisation: Processing data so that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such information, provided that such additional information is kept separately

with technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

- Representative: Person established in EU, designated by DC/DP to represent them with regard to their respective obligations.
- Supervisory Authority (DPA): This means an independent public authority which is established by a Member State pursuant to Article 51. In most cases, the supervisory authority will be the authority currently responsible for data protection measures. In Ireland, it is the Data Protection Commissioner's Office.

➢ **PRINCIPLES (ART. 5.1) PERSONAL DATA MUST BE**:

i. … processed lawfully, fairly and transparently.
ii. … can only be collected for specified, explicit and legitimate purposes.
iii. … adequate, relevant and limited to what is necessary for processing.
iv. … accurate and kept up to date.
v. … kept in a form such that the data subject can be identified only as long as is necessary for processing.
vi. … processed in a manner that ensures its security.

➢ **APPLICABILITY**

- Organisations within & outwith the EU. Extensive reach for liable in the event of a data breach.
- Potentially protects information of all "natural persons, whatever their nationality or place of residence."
- Personal data is: Information relating to an identified or identifiable natural person ('data subject' DS). An identifiable 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- This extended list of identifiable characteristics means that a great deal of anonymised data may no longer be suitable for distribution or sharing in public. Organisations that distribute anonymised data need to be carefully assess whether the data can be linked – directly or indirectly – to the DS.

➢ DATA SUBJECTS' RIGHTS

- Increases the rights for DS. Balancing DS rights vs right to the free flow of data to support "the pursuit of economic activities."
- Organisations must ensure that they know what data they collect and how they use data. Restrictive rules exist on what can be done without specific consent.
- DS can seek judicial remedies against DC & DP. Also have the right to seek compensation for damages arising from any breaches. Gives DCs vested interest in ensuring the security of any personal data that they pass to a processor.
- Consent:
    - Generally, DC needs DS's consent to process their data. Limited circumstances where consent is not necessary.
      e.g. (1) generally revolve around legal requirements (such as in compliance with another law, or to protect the rights of DS),

      (2) DS consent is provided through a contract they have with a third party.
    - Consent must be clear and unambiguous consent before processing personal data. "Silence, pre-ticked boxes or inactivity" are NOT consent. Processing cannot proceed unless DS has consented to every processing activity.

      If you wish to carry out six different actions with the subject's data, for instance, you need to ensure that the subject has consented to all of them.

    - Children under 16: Organisations need to obtain consent from the "holder of parental responsibility."
    - Consent possible with a tick-box, but consent document must be laid out in simple terms. "The request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."
    - Consent can be withdrawn. DC must provide a method that is "as easy to withdraw consent as to give it."
- Right to be forgotten:
    - (1) to have data erased under a number of circumstances (2) also must occur if DS withdraw consent for all of the processing for which the data is held.
    - Must take "reasonable steps" to erase any of the DS's data that might be public, such as in news articles or databases. Data Commissioner (DPA) will want to see that all appropriate technical and procedural measures to erase the data have been employed.
- Data Portability:
    - DSs can request a copy of any personal data held on them, and can also request that this information is transmitted to another data controller. Must be "structured, commonly used and machine-readable format."
    - Some organisations will already have appropriate contact with other organisations to facilitate the transfer of data - e.g. banks – and these contacts could be leveraged to streamline this process.

➢ LAWFUL PROCESSING

- Expanded in Article 6: (1) DS must have given consent or (2) processing is necessary for certain tasks, majority, require consideration of the data subject's interests.
- Permissible where "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, in particular where the data subject is a child."
    - Essentially makes lawful any reasonable processing in line with an organisation's interests, but must ensure that it does not otherwise threaten the interests, rights or freedoms of the data subject, is not in contravention of some other law or regulation, and 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.
- Will need to ensure that any processing without consent (or falling under one of the other stipulated conditions) is clearly permissible as part of the public interest.
    - In most cases, it will be simpler and safer to secure consent.
- Data can only be processed for limited purposes, to a minimal extent and accurately.
    - Tied to the requirements for transparency: the data subject must be aware of the nature of the processing, which will inform the 'limited purposes' and 'minimal extend.'
- Processing special categories of data (e.g. ethnicity, sexual orientation, health, etc.) is explicitly forbidden except in very specific circumstances.

➢ RETENTION OF DATA

- DS's right to be forgotten, hence the DC must erase all information held on them. Data can also only be retained for limited periods, which should be clear to the data subject at the point at which they consent. Not a hard and fast rule as some data could be held effectively indefinitely (e.g. public bodies for specific governmental purposes).
- While holding data, confidentiality and integrity must be secured – including against accidental loss, destruction or damage. Should be an extremely high priority for every organisation, e.g. due to compulsory data breach reporting.

➢ "ONE-STOP SHOP"

- GDPR intended to be a single scheme across the EU, to maintain a common market and support the free flow of information.
- EU Data Protection Board (EDPB) created to ensure that laws remain relatively consistent and with minimal impact on commerce.

- Member state will have Data Protection Authorities (DPA point of contact for GDPR issues). Intended to reduce the bureaucratic load for organisation dealing with data protection, anonymity and so on.
- Organisations will deal with the DPA in their primary jurisdiction. This will cover all cross-border intra-EU data processing.

➢ RECORDS OF DATA PROCESSING ACTIVITIES

- DC must retain record of its data processing activities. Record needs to contain, e.g. types of data is being processed, where it is processed, how it is processed and why it is processed.
- DP also required to keep a record of all processing carried out on behalf of DC.
- Records can be called upon by DPA at any time.

➢ DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

- Mandatory for technologies and processes that are likely to result in a high risk to the rights of data subjects.
- DC should ensure that DPIA is part of their risk assessment process regarding personal data and is in line with their data protection by design and by default strategies.
- Single DPIA can cover a set of similar processing operations with comparable risks.
- DPIAs can be outsourced.

➢ DATA PROTECTION BY DESIGN AND BY DEFAULT

- DPIAs usually relate to design phase of an application or process.
- GDPR makes mandatory 'privacy by design'. At the initial design stage, if any of processing could result in a loss of data protection, and have not been addressed 'by design and by default", then likely to be held liable in the event of a data breach.
- GDPR is technology neutral and does not specify how much security should apply, nor the specific measures to use – but a requirement "implement appropriate technical and organisational measures." Need to be able to prove to DPA that data protection was taken into consideration from the beginning.
- Where the risks were too great and then the processing should not take place. That is considering the state of the art, and a key part of data protection by default.

➢ DOCUMENTATION

- GDPR requires quite a bit of documentation. In addition to the explicit and implicit requirements for specific records (especially including proof of consent from data subjects), you should also ensure that you have documented how you comply with the GDPR so that you have some evidence to support your claims if the supervisory authority has any cause to investigate. If you suffer a data breach, for instance, being able to demonstrate that you have consistently applied best practice, that you have an audit trail showing that you notified them and any affected data subjects within the required timeframes, and that you have taken all the appropriate steps to mitigate the impacts of the data breach, will minimise the chance that you will be hit with a crippling fine.
- There are different documentation requirements for data controllers and data processors, but the onus for the documentation being correct will generally be on the controller, because they're likely to suffer the consequences regardless of who is at fault. If you are a controller with a number of processing functions outsourced, it's worth gaining assurances that these functions are appropriately documented.
- The following documentation is especially important, although, as noted above, it varies between data controllers and processors.
- Statements of the information you collect and process, and the purpose for processing HYPERLINK \| "39
- Records of consent from data subjects or their holder of parental responsibility HYPERLINK \| "40
- Records of processing activities under your responsibility HYPERLINK \| "41
- Documented processes for protection personal data – an information security policy, cryptography policy and procedures, etc.

➢ COMPLYING WITH GDPR

- Repercussions:
    - Could be fined up to €20 million or four percent of global annual turnover, whichever is greater. (e.g. Google > 1bn liability)
    - Certification bodies involved in certification schemes can face fines if they are found to be shirking their responsibilities. As such, it's possible for a single data breach to affect a large number of organisations – the data controller, any number of data processors involved in the data processors involved in the data breach, and the certification body that approved the data processing.
    - Because these administrative penalties can be applied so broadly, it is very important to understand what your own obligations and exposure are. You should be certain to consult a legal expert if you are concerned that you might not be in compliance with the law.
    - While fines from other regulators are unlikely to match the costs meted out under the GDPR, the compounding effects of other punitive measures could be significant.
    - Reputational damage could strip you of your customers, clients and suppliers.

- Ensuring that your organisation supports compliance with the Regulation from the very to will be critical to meeting your obligations – it would be difficult to implement all of the necessary measures without that level of support.

- Understanding your data - Flows and processes:
  - The first step toward compliance will be a data audit for an organisation, identifying the personal data they already hold, who it has been shared with and where it is now held, and to determine what must be done with that data in order to comply with the GDPR.
  - This data audit process will necessarily include reviewing existing processes for gathering personal data, ensuring there are clearly identified business and legal grounds for that collection, and ensuring that all related processes will comply with the new regulation.
  - Depending on the nature of your business, this could prove to be quite a broad exercise, showing points of egress and ingress where personal data goes out to a processor and then processed result returns. Also need to be quite clear about the information assets that actually constitute personal data – photographs, for instance, can be used to identify an individual and so will almost always be regarded as personal data.
  - Also consider where the data resides physically. If a Cloud solution is used, then will need to know where the Cloud supplier is based and, if they're not based in the EU, whether they are able to provide sufficient assurances that they meet the Regulation's requirements (including, crucially, legal protections for data subjects and the presence of effective legal remedies).
  - Should also note any physical records of personal data that might be kept, including HR records, historical records (assuming the subjects are still living) and so on.
  - Could carry out a DPIA in relation to information that you have already collected, in addition to any DPIAs necessary for future processing. This should highlight any weaknesses in your current operations that should be resolved.

➢ **ADDITIONAL CONSIDERATIONS**

- Changes to the 'Cookies Law'
  - Directive on Privacy and Electronic Communications or the (E-Privacy Directive) – was controversial when it came into force in 2011 and it has remained so.
  - GDPR mentions cookies once to clarify that they could be interpreted as an online identifier. Hence, is personal data and DS must consent.
  - The European Commission announced in 2016 that it would be evaluating the E-Privacy Directive. Possibly defining the exemptions for consent. Currently, under GDPR consent is not necessary, for instance, processing of personal data is lawful if: processing is necessary for the performance of a contract to which the DS is party or in order to take steps at the request of the DS prior to entering into a contract.

    - This allows e-commerce businesses to apply a cookie to track someone's purchases before they elect to actually buy them – the processing is a necessary step in the lead-up to a contract that the data subject will be entering (and providing consent for at that stage).
    - So, while it's possible that cookies will need to be more rigorously announced and consented to, it is equally possible that specific uses will be unaffected.
- The EU Network and Information Security (NIS) Directive:
    - Aims to establish national-level cyber security functionalities that will have an impact on ordinary businesses and other organisations.
    - Seeks to establish a "competent authority" for cyber security in each Member State. These authorities will be responsible for ensuring that national infrastructure is secure from cyber security threats and that the common citizen can have a degree of faith in the technologies they use daily. On top of this, a more secure national infrastructure is envisaged as having a positive economic impact because the stability and reliability of services will make it simpler to compete in the single digital marketplace.
    - Establishes another authority to whom threats and incidents will need to be reported. Because it's likely that the "competent authority" will end up being a branch of the security services, it could also result in a degree of censorship regarding details of data breaches, which could, in turn, be in breach of the Regulation.
- IP Addresses:
    - GDPR declares IP addresses to be personal data. For privacy campaigners, this is bothersome. On the one hand, the Regulation does attempt to protect this information where it could be used to identify someone, but at the same time it appears to assert that an IP address could be interpreted to indicate a specific geographical location. In the past court cases, it's been recognised that this is a misinterpretation of the way that IP addresses work, and several cases that have hinged on identifying individuals through their IP addresses have been thrown their IP addresses have been thrown out on the grounds that an IP address cannot prove either who was using the device at the time, or, in many cases, precisely where they are.
    - At the time of writing, a case is being argued in Germany that, on the grounds of privacy, website and application providers should not store dynamic IP addresses for longer than necessary to deliver content. Germany's Advocate General also argues that IP addresses be considered personal data and that they should therefore not be used for anything other than basic content delivery. While this is still going through the court system, and will likely be reviewed again some time before the Regulation comes into force, it does tend to indicate that organisations that use IP addresses to do anything other than deliver content will need to find new methods to do so, or ensure that consent is sought and gained.
    - It would also be quite reasonable to expect that other aspects of personal data will end up being argued in courts across the EU, and that the full scope of 'personal data' will evolve over time as a result.

➢ INTERNATIONAL TRANSFERS

- GDPR requires that protections are not undermined by the transfer (TBDFs). DCs must have safeguards to ensure DS rights and effective legal remedies are available in receiving country.
- US-EU Safe Harbour:
  - Framework: US organisations could attest that they adhered to seven principles and 15 frequently asked questions to meet the requirements of the DPD, which would then qualify them for certification under the framework and trouble-free access to the European market as a data processor. Dismantled in 2015.
  - EU-US Privacy Shield replaced Safe Harbour. Personal data exchanged under the auspices of this agreement will be governed by the GDPR.
  - EU Commission may also recognise some countries or international organisations as providing adequate protection for personal data. A list of these will be published and maintained, including noting where recognition has been removed. DCs/DPs can transfer data to those listed without any further authorisation or safeguards beyond those normally required under the GDPR.
- Binding Corporate Rules (BCRs):
  - DCs/DPs can transfer data if they put in place legally binding and enforceable arrangements to protect the rights of EU data subjects. Model binding corporate rules approved by the DPA is one such means.
  - Also can develop their own binding corporate rules to secure data when transferring to 3rd country. GDPR is very clear on what these rules must cover. Also, must be approved by DPA.
- Codes of conduct and certifications to international standards are also means by which DCs/DPs may be able to identify organisations that will provide appropriate safeguards. GDPR encourages DPAs to draw up codes of conduct and to encourage the use of data protection certifications.
- As DCs/DPs are accountable for data they are processing, any agreement to transfer that data to a third party, outside the arrangements identified in the GDPR, will be illegal. Important to consider when choosing Cloud providers.
- Highest penalties exist for bad practice in international transfers.

➢ ENCRYPTION

- DC/DP should already be encrypting mobile devices. Consideration should also be given to extending encryption to cover all of the data collection, processing and storage processes.
- For encryption standards, follow best practice. E.g. FIPS 140-compliant solutions.
- Ensuring that your solutions meet this standard will not only protect personal data in line with the Regulation's requirements, it may also allow you access to new markets or clients.
- Encryption beyond storage of personal data may also be valuable (or necessary) for establishing secure connections when personal data will be transmitted. Secure Sockets

Layer (SSL) encryption is no longer considered secure. Transport Layer Security (TLS) 1.2 or higher is really the new minimum for these connections.

➢ ACCOUNTABILITY AND THE BOARD

- A data breach should be on the Board's risk register, given the potential fines, the rights of DSS to bring cases/ claim compensation, and the prevalence and effectiveness of cyber-crime.
- DC will be accountable for failures of DCs, hence the Board must ensure that any DP are operating in accordance with the Regulation, regardless of the their jurisdiction.
- Besides the DPO, other roles will need a level of familiarity with the requirements of the GDPR - most HR staff, as well as middle and senior management in virtually any function that deals with personal data processed, stored or transmitted by the organisation.
- Training: Staff awareness training should support the more focused training that is applied to managers.

➢ DATA BREACHES

- Under DP Directive data breaches often happened without the DPAs being notified, nor the affected DSS. GDPR mandates informing both parties, with limited exceptions.
- Best practice is to ensure that there are processes in place to make these notifications in the event of a data breach.
- Reports must be made within 72 hours of the data controller becoming aware of the breach. Delays must be accompanied by an explanation.
    - Notification requires a specific format: including describing measures being taken to address the breach and mitigate its possible side effects.
    - Where high risks to the rights and freedoms of data subjects, then DSS must be contacted "without undue delay".
    - NOT necessary: if appropriate protective measures are in place to eliminate danger to data subjects. e.g. encryption.
- Incident response and breach reporting processes should be expanded to cover all potential cyber breaches. Continual testing and maintenance of these processes will be important to ensure that the 72-hour deadline is met - along with appropriate actions to protect data subjects' rights. (ISO27001 management systems covers this).

➢ DATA PROTECTION OFFICER (DPO)

- Required if: (1) data is processed by a public authority or body, (2) core activities consist of processing operations that require regular and systematic monitoring of data subjects on

a large scale, (3) activities consist of processing large quantities of special categories of data.

- Some companies will appoint a DPO even if they're not strictly required to - it's quite possible that an organisation's ordinary business will one day spike or adjust slightly, which will suddenly require a DPO. Requirements imposed by the GDPR makes the appointment of an appropriately qualified person to this role a sensible risk-containment step.
- Group of DCs/DPs may share a single DPO as long as they are "easily accessible from each establishment".
- DPO can be employed under a service contract.
- DPO must be qualified for the role on the basis of expert knowledge of data protection law and practices. The role must report directly to top management, to ensure that data protection remains a key concern for the Board and senior managers.
- DPO's duties include: (1) ensuring that organisation complies with GDPR. (2) offer advice, monitor DPIAS and (3) be the immediate contact for the DPA. DPO's name and contact details must also be published by the organisation e.g. on website privacy policies.
- DPOS need to be more than legal experts - need qualifications to handle the operational requirement to demonstrate appropriate organisational and administrative measures.

➢ DC/DP CONTACTS

- DP must provide "sufficient guarantees to implement appropriate technical and organisational measures" to comply with GDPR ensuring DS's rights are protected.
- Requirement moves down the supply chain, DP cannot engage a second DP without DP's explicit authorisation. Also, 2nd DP has to supply the same guarantees.
- Contractual arrangements must be reviewed and updated. Ensure that responsibilities and liabilities between DC and DP are defined. Must document responsibilities to ensure no confusion, and may have to accept that the increased risk levels and requirements for data protection measures may impact service costs.
- Certifications to international standards, e.g. ISO 27001 are recognised as effective to demonstrate appropriate technical and organisational measures have been implemented.

Part B

Data Protection Impact Assessment (DPIA)

➢ WHAT IS IT?

When your organisation collects, stores, or uses personal data, the individuals whose data you are processing are exposed to risks. Risks include data being stolen or inadvertently released and used by criminals to impersonate the individual DPIA is designed to identify & minimise these risks as far and as early as possible. A vital tool for negating risk, and for demonstrating compliance with the GDPR.

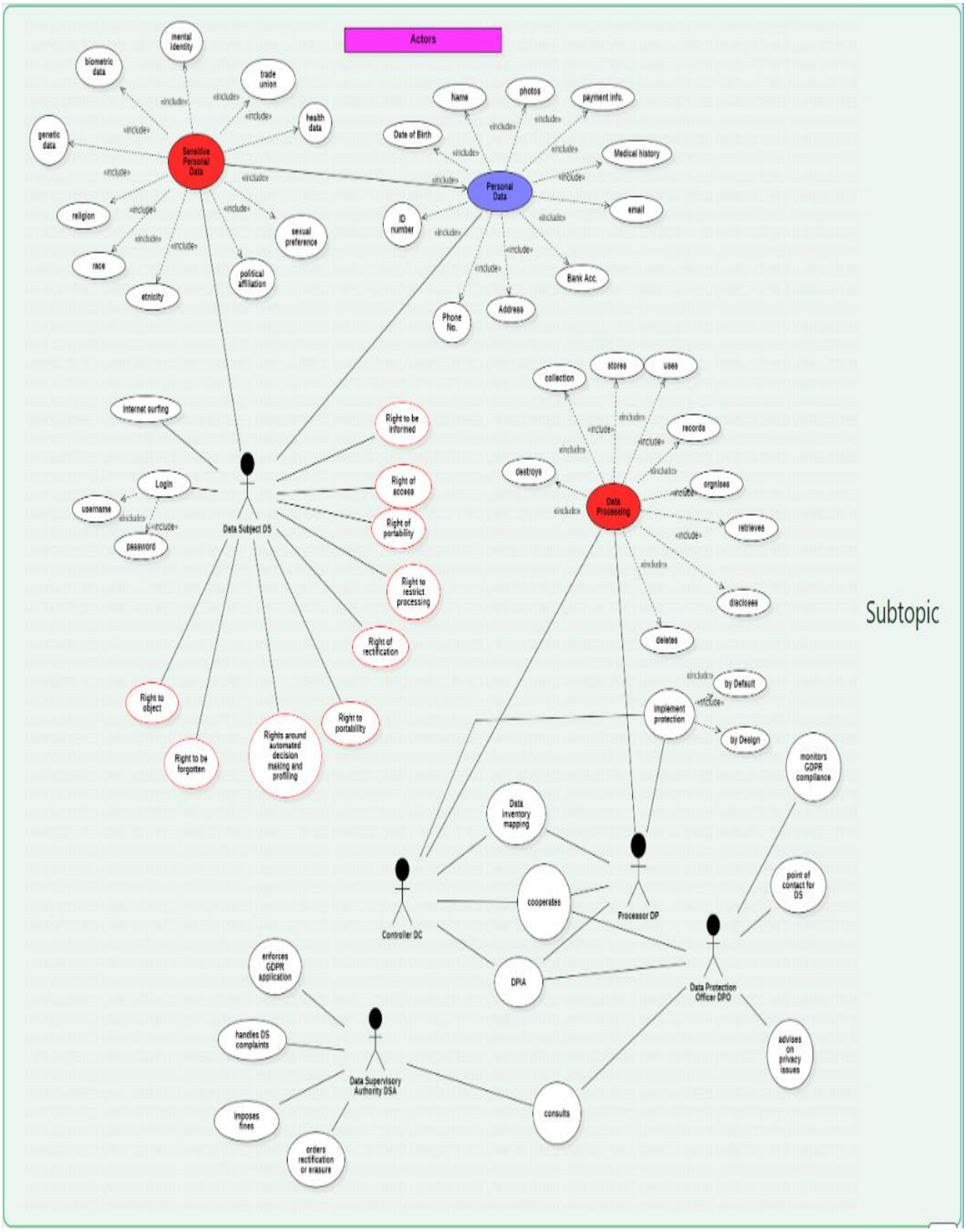
➢ KEY POINTS

- Under the GDPR, DPIAs will be mandatory for any new high risk processing projects.
- The DPIA process will allow you to make informed decisions about the acceptability of data protection risks, and communicate effectively with the individuals affected.
- Not all risks can be eliminated, but a DPIA can allow you to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks, and assess the viability of a project at an early stage.
- If a DPIA does not identify mitigating safeguards against residual high risks, the Data Protection Commissioner must be consulted.
- Good record keeping during the DPIA process can allow you to demonstrate compliance with the GDPR and minimise risk of a new project creating legal difficulties.

➢ BENEFITS

- Can demonstrate that your organisation complies with the GDPR thus avoiding sanctions.
- Fosters confidence in the public by improving communications about data protection issues. promoting confidence that user privacy rights are not being violated.
- Meeting the "data protection by design" standard for new projects.
- Reducing operation costs by optimising information flows & eliminating unnecessary data collection and processing. Reducing DP related risks to your organisation.
- Reducing the cost and disruption of data protection safeguards by integration at earlier stage.
- Promoting data protection by default, where service settings must be automatically data protection friendly.

- **GDPR MAIN ACTORS**



➢ WHEN IS ONE NEEDED?

- Mandatory where processing "is likely to result in a high risk to the rights and freedoms of natural persons".
    - Relevant when a new data processing technology is being introduced.
    - Even if not mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law.

- Examples of "likely to result in high risks":
    - "A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling."
    - "Processing on a large scale of special categories of data."
    - "A systematic monitoring of a publicly accessible area on a large scale."

- Article 29 Working Party has set forth the following criteria to consider:
    - Evaluation or scoring, including profiling and predicting, especially "from aspects concerning the data subject's performance at work, economic situation, health,…"
    - Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers.
    - Automated decision making with legal or similar significant effect.
    - E.g. the processing may lead to the exclusion or discrimination against individuals.
    - Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area"
    - E.g. where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).

- Sensitive data: this includes special categories of data (e.g. information about individuals' political opinions), as well as personal data relating to criminal convictions or offenses.

E.g. would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be considered as very intrusive.

- Data processed on a large scale: the GDPR does not define what constitutes large-scale, though provides some guidance. Recommends that the following factors be considered:

- The number of data subjects concerned, either as a specific number or as a proportion of the relevant population.
- The volume of data and/or the range of different data items being processed.
- The duration, or permanence, of the data processing activity.
- The geographical extent of the processing activity.
- Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes
- Data concerning vulnerable data subjects: the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data.
- E.g.: employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management.
- E.g.: children can't be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data.

- Innovative use:

  - e.g. combining use of finger print and face recognition for improved physical access control, etc.
  - The GDPR makes it clear that use of a new technology can trigger the need to carry out a DPIA. a new technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. the personal and social consequences of the deployment of a new technology may be unknown.
  - A DPIA will help the data controller to understand and to treat such risks.
  - E.g: "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy.

- Data transfer: across borders outside the European Union.

➢ **<u>DPIA STEPS INVOLVED</u>**

Annex 2 - Criteria for an Acceptable DPIA

The WP29 proposes the following criteria that data controllers can use to assess whether a DPIA, or a methodology for conducting a DPIA, is sufficiently comprehensive to comply with the GDPR:

1. **Systematic Description of Processing (Article 35(7)(a))**:
   - A systematic description of the processing is provided.
   - The nature, scope, context, and purposes of the processing are considered (recital 90).
   - Personal data, recipients, and the period for which the personal data will be stored are recorded.

- A functional description of the processing operation is provided.
- The assets on which personal data rely (including hardware, software, networks, personnel, and physical transmission channels) are identified.
- Compliance with approved codes of conduct is taken into account (Article 35(8)).

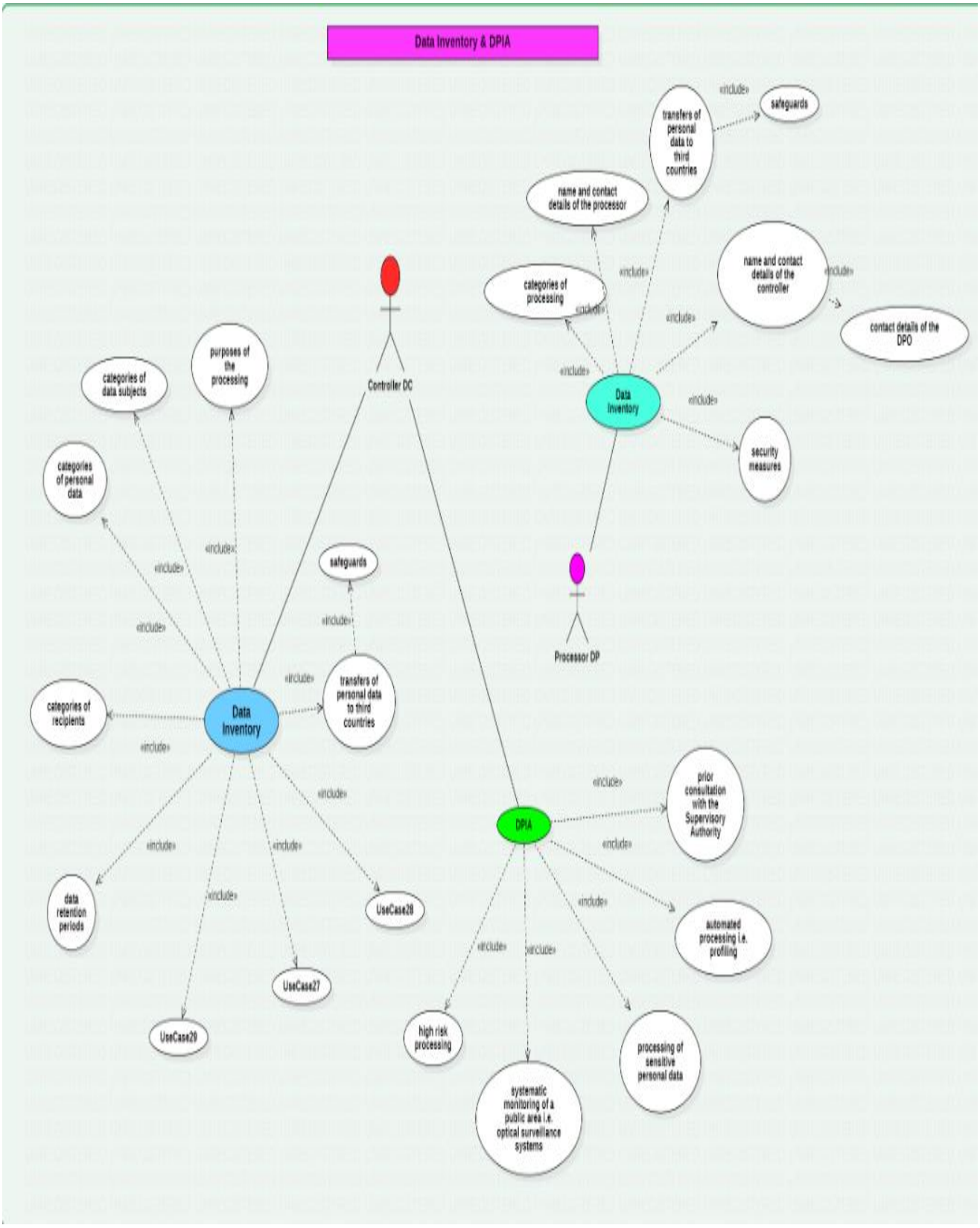
2. **Assessment of Necessity and Proportionality (Article 35(7)(b))**:
    - Measures necessary to comply with the Regulation are identified (Article 35(7)(4) and recital 90), considering:
        - Proportionality and necessity of processing based on specified, explicit, and legitimate purposes (Article 5(1)(b)).
        - Lawfulness of processing (Article 6).
        - Adequate, relevant, and limited data (Article 5(1)(c)).
        - Limited storage duration (Article 5(1)(e)).
    - Measures contributing to the rights of data subjects include:
        - Information provided to the data subjects (Articles 12, 13, and 14).
        - Right of access and to data portability (Articles 15 and 20).
        - Right to rectification and erasure (Articles 16, 17, and 19).
        - Right to object and restriction of processing (Articles 18, 19, and 21).
        - Relationships with processors (Article 28).
        - Safeguards surrounding international transfers (Chapter V).
        - Prior consultation (Article 36).

3. **Management of Risks to the Rights and Freedoms of Data Subjects (Article 35(7)(c))**:
    - The origin, nature, particularity, and severity of the risks are evaluated (cf. recital 84). For each risk (e.g., illegitimate access, unauthorized modification, and data loss), consider:
        - Risk sources (recital 90).
        - Potential impacts on the rights and freedoms of data subjects in cases of events, including illegitimate access, unauthorized modification, and data loss.
        - Identification of threats that could lead to illegitimate access, unauthorized modification, and data loss.
        - Estimation of likelihood and severity (recital 90).
    - Measures to address those risks are determined (Article 35(7)(d) and recital 90).
    - Interested parties are involved:
        - The advice of the Data Protection Officer (DPO) is sought (Article 35(2)).
        - The views of data subjects or their representatives are solicited, where appropriate (Article 35(9)).

➢ WHO SHOULD BE INVOLVED?

- The data controller is responsible for ensuring the DPIA is carried out.
- The DPIA should be driven by people with appropriate expertise and knowledge of the project in question, normally the project team.
- If your organisation does not possess sufficient expertise and experience internally, or if a particular project is likely to hold a very high level of risk or affect a very large number of people, you may consider bringing in external specialists to consult on or to carry out the DPIA.
- A wide internal consultation process can benefit the DPIA, as some data protection risks will only be apparent to individuals working on specific aspects of the project. It will also allow you to gain feedback from those whose work will be affected by the project after implementation, such as engineers, designers and developers, who will have a practical knowledge of the operations. Involving your organisations public relations team will allow for effective communication of the DPIA's outcomes to external stakeholders.
- Seek the advice of the DPO. This advice and the decisions taken should be documented as a part of the DPIA process. If a data processor is involved in the processing, the data processor should assist with the DPIA and provide any necessary information.
- The data controller is bound to "seek the views of data subjects or their representatives", "where appropriate" in carrying out the DPIA. In some cases, the data subjects may be people within the organisation. Seeking the views of data subjects will allow the data controller to understand the concerns of those who may be affected, and to improve transparency by making individuals aware of how their information will be used.
- The views of data subjects can be sought through a variety of means, depending on the context. Staff could be consulted through a trade union; customers could be consulted by means of a survey. If the data controller's final decision differs from the views of data subjects, the reasons should be recorded as a part of the DPIA. If the data controller does not feel it appropriate to seek the views of data subjects, the justification for this should be documented.

- **INVENTORY & DPIA**



➢ WHEN IN A PROJECT LIFECYCLE?

- It is generally good practice to carry out a DPIA as early as practical in the design of the processing operation.
- It may not be possible to conduct a DPIA at the very inception of the project, as project goals and some understanding of how the project will operate must be identified before it will be possible to assess the data protection risks involved.
- For some projects the DPIA may need to be a continuous process, and be updated as the project moves forward.
- The fact that a DPIA may need to be updated once processing has actually started is not a valid reason for postponing or not carrying out a DPIA.

- **PRIVACY BY DESIGN & BY DEFAULT**