DATA PROTECTION NETWORK

PRIVACY PARTNERSHIP LAW

PrivacyX Consulting

Legitimate Interests Guidance and Assessment

Guidance on the use of Legitimate Interests under the General Data Protection Regulation (Regulation (EU) 2016/679) and UK GDPR

Version 3.0 published November 2024

Contents

Introduction

The purpose of this Guidance is to help commercial and not-for-profit organisations to understand the concept of legitimate interests and assess whether or not they can rely on legitimate interests as a lawful basis for processing personal data under the GDPR. The guidance sets out a clear methodology for conducting a documented assessment, known as Legitimate Interests Assessment (or LIA).

Any reference to GDPR in this guidance is intended to cover both the General Data Protection Regulation (Regulation (EU) 2016/679) and UK GDPR.

In this version 3.0, published November 2024, we have updated the previous content and provided examples of emerging use cases, including using legitimate interests as the lawful basis for processing personal data within an Artificial Intelligence (AI) system. We also reference an initiative to develop guidance and a Legitimate Interests Assessment (LIA) template specifically for assessments involving the use of Artificial Intelligence (AI) from the Information Accountability Foundation (IAF), on which DPN collaborated.

UK and EU Data Protection Authorities have published guidance on legitimate interests, as has the European Data Protection Board. For recent developments and news about Legitimate interests please visit our website: *Legitimate Interests*

The GDPR sets out six lawful bases (also known as 'legal bases') for processing personal data in Article 6. Controllers need to select the most approriate lawful basis for each specific processing activity.

- **CONSENT** - the individual has given their Consent to the processing of their personal data.
- **CONTRACTUAL** - processing of personal data is necessary for the performance of a contract to which the individual is a party or for the Controller to take necessary pre-contractual steps.
- **LEGAL OBLIGATION** - processing of personal data is necessary for compliance with a legal obligation to which the Controller is subject.
- **VITAL INTERESTS** - processing of personal data is necessary to protect the vital interest of the individual or of another individual.
- **PUBLIC TASK** - processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- **LEGITIMATE INTERESTS** - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Under GDPR, Article 6 1(f)

'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Under Recital 47

'The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.'

Due to challenges meeting the specific requirements of other lawful bases, such as the conditions for valid consent or the necessity test for performance of a contract, many organisations look to legitimate interests to provide more flexibility, and a lawful basis which may be more sustainable in the long term.

This guidance considers a wide spectrum of processing activities which may be covered by legitimate interests. Our intention is to help organisations understand the circumstances in which legitimate interests may apply and provide an assessment framework which can be applied to each organisation's specific circumstances.

Although the ability of public authorities to rely on legitimate interests is restricted under Article 6 of the GDPR, it may be possible for these bodies to rely on this lawful basis for tasks other than public tasks or those required in the public interests of a public authority.

This initiative was led by Data Protection Network (*www.dpnetwork.org.uk*). The information provided in this guidance represents the views of the Data Protection Network, including the views of the DPN Legitimate Interests Working Group of 2017/18 - a group comprising representatives from a wide range of companies and institutes operating in the UK and further afield who collaborated to produce versions 1 and 2.

Three-stage test for legitimate interests

There are three key conditions which need to be met when seeking to rely on legitimate interests as the lawful basis for processing. This is often referred to as the 'three-stage' test and comprises of:

1. **Identify the purpose of processing and if the interests pursued are legitimate,**
2. **Establishing that the processing is 'necessary', and**
3. **Conducting the balancing test.**

1. Identify the purpose of processing and if the interests pursued are 'legitimate'

The first stage is to identify the purpose (or purposes) for processing personal data and why it's important to your organisation, as a controller.

A legitimate interest may be elective or business critical; however, even if the interest is obvious and legitimate, it must be clearly articulated and communicated to the individual.

Legitimate interests can be those of the controller or a third party to whom the personal data may be disclosed. It's possible several parties may have a legitimate interest in processing the personal data and while you may only need to identify one legitimate interest, all relevant interests should be considered. Your Legitimate Interests Assessment (LIA) would only cover your relevant processing and any disclosure of the personal data. A third party would have to conduct their own assessment for their own processing purposes.

An 'interest' can be considered as 'legitimate' if it can be pursued in a way which complies with data protection and other laws. Some interests are likely to be legitimate because they're integral to corporate governance or related legal compliance issues, particularly where there's no legal obligation to comply with but the processing is essential to make sure the organisation meets external or internal governance obligations. Other interests are legitimate because they're a part of the organisation's routine activities and other lawful bases for processing are not practical or appropriate.

An 'interest' is the broad stake an organisation may have in the processing, or the benefit the organisation or society might derive from it. It must be real and not too vague. For example, many businesses want to make a profit but this does not mean this broad objective is a legitimate interest in and of itself.

It should be noted if your processing operations are solely in the UK, the Information Commissioner's Office guidance is open to wider public interests, whereas the European Data Protection Board draft guidance published in October 2024 is more cautious about whether wider public interests are relevant.

Regardless of the importance of the processing activity to the organisation, an assessment must be made to make sure the processing meets the threshold required to rely on legitimate interests as the lawful basis.

Of note is a significant ruling in October 2024 by the Court of Justice of the European Union (CJEU) in which it confirmed legitimate interests can include purely commercial interests. However, the CJEU stressed the need to determine necessity, conduct a balancing test, implement transparency measures and make sure individuals can object at any time. ***(CJEU case reference: C-621/22)***

2. Establish if the processing is necessary

Organisations should consider whether the processing of personal data is truly necessary for the pursuit of its commercial or business objectives.

The meaning of the term 'necessary' may be interpreted slightly differently in Europe than it is in the UK. The UK ICO legitimate interests guidance states: *"This doesn't mean that it has to be absolutely essential, but it must be a targeted and proportionate way of achieving your purpose."* Whereas the European Data Protection Board (EDPB) draft guidance states: *"The controller may rely on this legal basis only if it has also assessed and concluded that the envisaged processing is strictly necessary for pursuing such a legitimate interest..."*. Any organisation operating in both the EU and UK, or solely in the EU may wish to take heed of the EDPB guidance.

It may be helpful to ask: *"Is there another way of achieving this?"*

- If there isn't any alternative to achieve the interest(s), then clearly the processing is necessary; or
- If there is another way but it would require disproportionate effort, then you may determine the processing is still necessary; or
- If there are multiple ways of achieving the objective, a Data Protection Impact Assessment (DPIA) could be used to identify the least intrusive processing activity; or
- If the processing is not necessary, then legitimate interests cannot be relied on as a lawful basis for that processing activity.

In practice, legitimate interests can only be relied upon as a lawful basis of processing to the extent such activity is 'necessary' (for the purpose of the controller's or a third party's legitimate interests.

3. The balancing test

The GDPR provides protection for individuals by requiring that all their relevant 'rights and freedoms' and 'interests' are taken into account, and weighed against the interests of the controller.

Note people's rights, freedoms and interests are not limited to their privacy rights but also include other fundamental human rights.

An organisation can only rely on legitimate interests where the interests, and the rights and freedoms of the individual whose personal data will be processed have been evaluated, and these do not override the organisation's legitimate interest.

Balancing test considerations

The balancing test must be conducted fairly and organisations should give due regard and weighting to the interests, and the rights and freedoms of individuals. There are several factors to consider when evaluating whether an individual's rights would override an organisation's legitimate interest (or that of a third party). These include:

- the categories and types of personal data
- the context, nature and means of processing
- the nature of the interests of the individual
- the rights and freedoms of individuals
- the impact of processing
- any safeguards in place, or which could be put in place

1. The categories and types of personal data

Controllers need to consider the impact of processing certain types of personal data and the people it relates to. For example, special category data and data relating to children or other vulnerable people require additional protection under the GDPR. Does the processing involve other data which individuals may consider more private? For example, location data or financial information? Data which is more private or sensitive has the potential to elevate negative impact and/or harm to the individual. This is likely to give additional weight to the interests, rights and freedoms of individuals.

2. The context, nature and means of processing

The context of the relationship between the organisation and the individual is a key element in understanding the legitimacy of the processing activity. Is there a direct or indirect relationship between the parties? A direct relationship with the individual is not essential for relying on legitimate interests although the requirement to inform individuals that you have obtained their data from a third party would have to be taken into consideration.

Where there is a direct relationship, consider whether there may be an imbalance of power between you and the individual. For example, between an employer and employee, or organisation and patient. The nature of the relationship should be weighed against the necessity of the processing and the impact on the individual.

The specific means of data processing can impact on the rights and interests of the data subject. To give a few examples:

- the degree of automation (e.g. within an AI model) and the level of human involvement and oversight
- the involvement of the use of Artificial Intelligence (AI)
- the scale of the processing; how much data, how many individuals etc
- whether combined data sets are being used

3. The nature of interests of the individual

The interests of individuals include, but are not limited to, matters such as personal, financial and social interests. Organisations also need to assess the reasonable expectations of the individual. Would or should they reasonably expect the processing to take place? If they would, this is likely to add weight to the organisation's interests. If they have no expectation, then the impact is greater and more weight is given towards the individual in the balancing test.

4. The fundamental rights and freedoms of the individual

While people have a right to data protection and privacy, there are also other fundamental rights and freedoms. For example the right to freedom of thought and expression, freedom of assembly and association, the right to liberty and security, plus other rights and freedoms protected by law and ethics. A balancing test should consider all these other fundamental rights and freedoms (where relevant).

Looking specifically at the GDPR, individuals are provided with specific privacy rights; many of which apply whatever the lawful basis for processing (although there are some exceptions).

- The right to be informed how personal data is processed - individuals have a right to be informed where processing relies on legitimate interests, and of their right to object to such processing
- The right of access to their personal data
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

5. The impact of processing

A crucial part of the balancing test is assessing the impact of the processing. This means assessing any positive or negative impacts on the individual, any bias or prejudice to the controller, third party or to society of not conducting the processing. The likely impact and severity of any impact on individuals need to be explored.

A much more compelling justification will be required if there is any likelihood of harm occurring. Data protection harms can arise when personal data is used, misused or lost. They can also arise when individuals have an inability to exercise their privacy rights. Harms may have a variety of impacts on individuals, which can range from financial loss, emotional distress and even physical harm. The UK ICO says *"causes and events in isolation are not harms, it is the resulting negative consequences or impacts of events that are harms."* The ICO accepts identifying harms can be challenging to robustly quantify. For more information see the *ICO Overview of Data Protection Harms*.

Factors which could affect the impact of processing include:

- The status of the individual (with respect to the controller or third party) – a customer, a minor, an employee, or other.
- The status of the controller - such as, whether an organisation is in a dominant market position or has undue influence over the individual.

Organisations should aim to provide evidence of the impact the processing could have, particularly in more complex cases. This could include documented evidence of the benefits. Evidence can be drawn from both internal and external stakeholder consultations. For example, in a highly competitive or regulated industry (such as financial services), enhanced customer segmentation may be a more crucial activity for customer acquisition and retention than in other sectors.

6. Safeguards

Safeguards may include a range of technical and organisational measures or controls which are in place, or which could be put in place, to protect the individual or to reduce any risks or potentially negative impacts of processing. It may not be necessary to completely eliminate risk, but appropriate safeguards should reduce it to an acceptable level.

Examples of safeguards include (but are not limited to):

- privacy by design measures
- data minimisation
- de-identification, pseudonymization or anonymization
- providing extra transparency or explainability
- restricting user access rights
- limited data retention
- opt-out options
- putting data out of reach
- technical security measures, such as multi-factor authentication encryption, hashing, salting
- other technical or organisational measures to protect personal data or to prevent or minimise harm

In more complex assessments, it will be important to be able to cite evidence of the efficacy of safeguards i.e. can you demonstrate a specific safeguard will produce the intended result?

7. Other related risk assessments

The controller may be required to conduct other risk assessments separately or in parallel with an LIA to enable compliance with relevant laws. To name a few:

- Data Protection Impact Assessment (DPIA)
- Fundamental Rights Impact Assessment (FRIA) under EU AI Act
- International Data Transfer Impact Assessments (or Data Transfer Risk Assessments under UK GDPR)

Clear information from other assessments may need to be referenced in your LIA, in particular under the Balancing Test (e.g. assessment of potential harms to individuals explored in other assessments).

How to conduct a Legitimate Interests Assessment (LIA)

If an organisation wishes to rely on legitimate interests, it must carry out an appropriate assessment, often referred to as a Legitimate Interests Assessment (LIA).

Why document the assessment?

It's advisable, to ensure compliance with the accountability principle under the GDPR, to keep a record of any LIA conducted, including reasons for reaching your conclusions. This may be required as evidence in future.

- LIAs may need to be disclosed to Data Protection Authorities in the event of an investigation. Organisations need to be ready to demonstrate they've fully considered the purpose and necessity of processing, and came to the decision the individual's interests, and their rights and freedoms did not override the organisation's interests.
- LIAs may need to be provided to other organisations as part of due diligence in the event of a sale or acquisition. The controller to whom personal data is disclosed may need to review the LIAs and update them where processing activities will differ. Additional requirements set out in the GDPR may also need to be met, such as notification of changes to processing.

Who should conduct the LIA?

The organisation should decide who should be involved in conducting an LIA and what their roles are. Ideally, a data protection subject matter expert should lead the assessment process, in conjunction with the relevant stakeholders.

Where practical to do so, there should be a separation of responsibilities between the person or teams who 'own' the processing activity (e.g. the 'first line of defence') and those who act in an advisory capacity to the organisation (e.g. a Data Protection Officer). However, where this is not possible, an individual with appropriate knowledge and seniority should be accountable. In any event, conflicts of interest should be avoided. The Balancing Test must be conducted fairly before a decision is made on the lawfulness of processing.

What if the balancing test does not come out in favour of the controller?

If the LIA process leads to a negative outcome (i.e. the controller cannot rely on legitimate interests for the processing operation), the organisation may wish to reduce the scope or refine the nature of the processing operation, or put in place compensating controls, then re-apply the balancing test. If changes are not practical and the outcome of the LIA is still negative, an alternative lawful basis must be found, or the processing activity should not proceed.

What if the scope of the processing activity changes?

An LIA should be revisited if the organisation becomes aware of any material changes. The organisation may wish to set review periods for LIAs as a reminder. It may be necessary to conduct a new LIA if the purposes of the processing change. Please see the LIA Template (Appendix B)

What if individuals are alleged to be engaged in illegal activities?

An individual who may be engaged in alleged illegal activity, or whose data is processed in relation to an age restricted or regulated environment, still has rights and freedoms. However, where the processing activity addresses illegal activity (such as protection against security threats or fraud prevention), the legitimate interests of the organisation may be compelling.

LIA Template

Our LIA template has been specifically developed to help organisations carry out an assessment. This template can be adapted to suit the sector and industry of your organisation.

While this LIA will help you conduct an assessment and determine if legitimate interests can be relied on, conclusions will be subjective and should be based on the experience and judgement of the individual or individuals completing the assessment. Any assumptions should be clearly stated.

DOWNLOAD LIA TEMPLATE

Individuals' privacy rights & legitimate interests

People have the right to be informed about how their personal data is processed. Transparency is a key principle underpinning GDPR. Other privacy rights can differ depending on which lawful basis for processing is being relied on.

Right to be informed

The GDPR clearly stipulates specific privacy information must be provided to individuals. Article 12 states this must be provided in a '*concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*'

Article 13 goes on to specifically mention privacy information provided to individuals should include details about a controller's reliance on legitimate interests, and the need to explain what those legitimate interests are.

It's also a requirement to notify individuals of their right to object to processing under this lawful basis. This legal requirement is likely to be covered in a Privacy Notice.

Organisations can refer to guidance from Data Protection Authorities on privacy notices. For example the UK ICO *Right to Be Informed Guidance*.

Right to object

Not only should individuals be informed about processing based on legitimate interests, but they should also be informed about their right to raise an objection. Organisations must then assess an individual's objection; either fulfilling it, or justifying why they won't be. In relation to direct marketing, an objection must be upheld, as this is an absolute right. However in other cases such as fraud prevention or network and information systems, an objection may not be considered enough to override the organisation's legitimate interests.

Right to erasure

This is not an absolute right, but it would apply if the organisation cannot justify the legitimacy of the processing. It would also apply where the personal data is no longer required for the purpose it was originally collected.

Right of data portability

This right does not extend to personal data processed on the basis of legitimate interests.However, you should refer to official guidance from any relevant Data Protection Authority regarding the scope of the right to portability, particularly in relation to *'observed data.'*

Rights in relation to automated decision-making (including profiling)

As per GDPR Article 22, legitimate Interests cannot be used for automated decision-making (ADM) which produces legal or similarly significant effects concerning the individuals the processing relates to. However, legitimate Interests could potentially be used for partially automated decision-making or profiling. This may be useful in the context of the growth of AI.

Artificial Intelligence (AI) and legitimate Interests

Many organisations may seek to rely on legitimate interests as their lawful basis for using personal data in the development, training or deployment of artificial intelligence (AI) systems or applications. Personal data may be an input or an output from an AI system.

Legitimate interests may be the most flexible lawful basis, but this does not mean it will automatically be appropriate in all these situations. The 3-stage test is likely to be more complex for AI than many other types of processing. Consideration should be given to various aspects of AI processing, such as:

- **Purpose** – identifying the purpose of processing and if the interests pursued via AI are genuinely legitimate. For which aspects of the AI lifecycle do you wish to rely on legitimate interests, e.g. development, training and/or deployment? It will also be important to distinguish whether AI systems are trained using first, or third party, personal data.
- **Necessity** – confirming if the planned use of personal data using AI is truly necessary. Could the processing be carried out without using personal data? Is the training possible using anonymised or synthetic data? Could the personal data be minimised?
- **Balancing test** – weighing up the rights, freedoms and interests of individuals may be more complex when AI is used. In particular, appropriate safeguards will need to be confirmed if risks of fairness and bias are identified. Other safeguards, could include mechanisms to prevent the re-use of user inputs for AI training.

Legitimate interests may not be applicable if AI is used in a way which individuals would not expect (transparency is a key consideration), or which may cause unnecessary harm.

Data protection considerations will need to include the individuals whose personal data is used to train the system, and the impact the system, once deployed, has on the rights and freedoms of individuals and society.

Alignment with other assessments

Any framework for assessing legitimate interests in relation to AI will benefit from a multi-dimensional approach, to take into account all relevant interests and fundamental rights. The findings from all these assessments should be considered within your LIA. In particular, we would highlight:

- Data Protection Impact Assessment;
- Fundamental Rights Impact Assessment (FRIA) under EU AI Act
- Transfer Risk Assessment (aka Transfer Impact Assessment);
- Other risk assessments required to comply with laws in other territories.

Organisations will need to take a broader view than solely data protection. For example, to meet the requirements of the EU AI Act, a Fundamental Rights Impact Assessment (FRIA) requires a description of the organisation's processes in which a high-risk AI system will be used, in line with its intended purposes. Organisations should take into account all interests and fundamental rights found in the Charter of Fundamental Rights of the EU (EU Charter) and the UN Universal Declaration of Human Rights (UN Charter).

The findings from all these assessments should be considered within your LIA.

AI guidance from Information Accountability Foundation (IAF)

The Information Accountability Foundation (IAF) have developed a model normative framework: *Assessments for an AI world: Legitimate Interests Assessment.* This provides useful guidance for organisations wishing to rely on legitimate interests for AI, which incorporates a multi-dimensional approach and includes its own LIA template designed specifically for AI assessments. DPN collaborated with IAF on this project.

AI guidance from Data Protection Authorities

UK, EU and other Data Protection Authorities are producing AI-related guidance. The UK ICO's

ICO example

An organisation seeks to rely on legitimate interests for processing personal data for the purposes of training a machine learning model. Legitimate interests may allow the organisation the most room to experiment with different variables for its model.

However, as part of its legitimate interests assessment, the organisation has to demonstrate that the range of variables and models it intends to use is a reasonable approach to achieving its outcome. It can best achieve this by properly defining all of its purposes and justifying the use of each type of data collected – this will allow the organisation to work through the necessity and balancing aspects of its LIA. Over time, as purposes are refined, the LIA is revisited.

For example, the mere possibility that some data might be useful for a prediction is not by itself sufficient for the organisation to demonstrate that processing this data is necessary for building the model.

Please see *DPN's website* for latest DPA guidance and updates.

GDPR examples of legitimate interests

GDPR provides some examples of when an organisation may have a legitimate interest. These are set out in recitals 47 to 50. Such legitimate interests would need to be confirmed by conducting a LIA.

1. **DIRECT MARKETING** – processing for direct marketing purposes under legitimate interests is specifically mentioned in the last sentence of Recital 47 which states; *"The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest"*
2. **REASONABLE EXPECTATIONS** – if individuals have have a reasonable expectation that an organisation will process their person data for a specific purpose, or purposes, will help the make the case for legitimate interests when conducting the balancing test.
3. **RELEVANT & APPROPRIATE RELATIONSHIP** – there is a relevant and appropriate relationship between the individual and the organisation in situations where the individual is a client or in the service of the organisation. However, this does not mean there will always be a legitimate interest in processing an individual's data. Legitimate interests is more likely to apply when there is a direct 'appropriate' relationship with individuals because the processing is less likely to be unexpected or unwanted, so the balancing test will be easier. Recital 47 indicates it is more difficult to use legitimate interests when there is no pre-existing relevant relationship (although this is not ruled out).
4. **STRICTLY NECESSARY FOR FRAUD PREVENTION** – where the processing is strictly necessary for the purpose of preventing fraud. This could include verifying the registered address of the cardholder for a particular credit or debit card is the same as the cardholder's normal place of residence or work.
5. **ORGANISATIONAL** – where controllers are part of an organisational group or institutions affiliated to a central body that transmit personal data within that organisational group or to the central body. However, additional requirements on transferring personal data to a country outside the European Economic Area (EEA), or indeed outside the UK, must be complied with where relevant.
6. **NETWORK & INFORMATION SECURITY** – where the processing of personal data is strictly necessary and proportionate for the purposes of ensuring network and information security. An example of this would include monitoring user access to a computer network for the purpose of preventing cyber attacks.

Case studies and examples

There are a wide range of processing activities for which organisations may wish to consider relying on legitimate interests, subject to a LIA. This may be processing clearly for the individual's benefit, for the mutual benefit of both the individual and the controller (or a third party), where the organisation has a compelling interest in the processing and/or when there is a limited privacy impact on the individual.

Depending on the processing activity in question, the balancing test used to assess legitimate interests may be very straightforward or more complex. In the case of the latter, documenting how the decision to rely on legitimate interests was reached will be crucial.

Case studies

The following case studies, provide an illustration of how the "3 stage test" might be addressed. These case studies would be subject to any organisation's own assessment.

- **A.** Employer using AI in psychometric testing
- **B.** Telematics
- **C.** Charity prospecting
- **D.** Membership postal communications

(A) EMPLOYER USING AI IN PSYCHOMETRIC TESTING

An employer wants to use enhanced psychometric testing as part of their recruitment procedures. The service provider uses AI in the psychometric solutions it provides.

Is this a legitimate interest?

The employer needs to carry out appropriate assessments for job applicants to make sure their qualifications and skills are genuine and to assess their suitability for the role they have applied for. Psychometric tests are used to help objectively assess relevant candidates' skills and abilities, in scientifically proven ways, whilst reducing the burden on the recruiting manager's time.

Consent may not be a suitable lawful basis for psychometric tests. It is possible that 'contractual necessity' may apply, however, the most practical lawful basis for this activity is may be legitimate Interests.

Is the processing necessary?

The processing is necessary to make sure candidates have the relevant skills, understanding and abilities appropriate to the role they are applying for.

The balancing test

Any processing of candidates' personal data should be proportionate and must not be outweighed by the interests and fundamental rights of individuals. In this situation, it is judged psychometric tests are beneficial to both the employer and candidate; it is mutually beneficial to ensure a good fit for job roles.

Concerns may arise over the use of AI, the risks of algorithms, the possibility of bias and the lack of human intervention. To justify this use of AI-driven tests, appropriate checks and balances need to be put in place.

Safeguards

In relying upon legitimate interests, safeguards should be put in place to minimise data collection, providing guidance to staff undertaking this activity.

Job applicants and employees must be notified of any use of profiling and/or automated decision making, so the relevant Privacy Notice for applicants should be updated before the psychometric tests commence. Where individuals have a right to object, a procedure needs to be in place to handle any objections which may be received. Alongside an LIA, a Data Protection Impact Assessment (DPIA) needs to be carried out for this activity and perhaps a separate AI Risk Assessment too.

(B) TELEMATICS

A company intends to use telematics on its fleet of driver operated vehicles. The telematics will perform a number of functions including:

- Promoting the safety of drivers using the vehicles;
- Processing traffic offences and incidents;
- Processing location and other data for both safety of the driver as well as protection of third parties in the event of a machine malfunction.

The processing will be carried out during working hours and in the context of the employment of the driver.

Is this a legitimate interest?

The use of telematics in this context is likely to be a legitimate interest for the organisation to ensure that vehicles being operated by their employees are being operated safely and in the correct manner.

Is the processing necessary?

The processing is necessary to ensure compliance with health and safety legislation. It is also important to ensure that the driver complies with the organisation's policies and processes relating to the use of its vehicles. Without vehicle telematics it would be difficult to carry out monitoring of the vehicles being operated by employees and their employer would instead be purely reliant on individuals adhering to the policies without any monitoring taking place. This could place road users at risk should breaches of policy take place and the business not becoming aware unless other road users reported them to the business.

The balancing test

The individual might not expect the use of telematics, but a process is in place to communicate the use of telematics to relevant employees, as part of their contract of employment and within their staff manual and training. The risk might be that the location data may identify the driver being somewhere they are not expected to be, or might infringe their human or data protection rights where they are being monitored outside of their working hours. That said, the system is developed with the facility to turn the monitoring off when the vehicle is being used for personal use.

However, if the processing did not take place unwarranted harm or distress to the individual could occur. For example, if there was an incident involving the vehicle, the safety of the individual and/or third parties could not be remotely safeguarded. The telematics are controlled centrally and cannot be controlled locally on the vehicle, although the organisation is looking to provide local control to ensure the individual can indicate when the telematics should operate (in line with company policy).

Safeguards

The organisation has in place suitable transparent notices to employees who are drivers of the vehicles. They restrict access to any personal data to a limited number of central employees who manage telematics information. It may be necessary to encrypt the telematics information during transition and to provide a mechanism for stopping the collection of personal data and special categories of personal data when the vehicle is being used outside business hours (if appropriate).

(C) CHARITY PROSPECTING

A charity has taken over an old cinema and is converting it into a new community theatre and arts centre. To fund the refurbishment and opening, they want to use prospect research to help identify new patrons, ambassadors, and potential major donors who are suitable to their cause and have the capacity to make substantial donations and philanthropic gifts.

Using legitimate interest as a basis for processing, they undertake research using publicly available information (such as from national and local press, as well as information from Companies House and the Charity Commission) to identify and inform appropriate professional approaches to individuals who are involved in charitable activity, have perhaps made previous philanthropic gifts, or are prominent in the field of arts, culture, and theatre.

Is this a legitimate interest?

The charity has a legitimate interest in seeking support for this project. For the charity to be able to do their work, they need to find new supporters and raise money. For significant projects, it is prudent to scope the philanthropic landscape to determine whether there are sufficient potential funders to feasibly secure enough funding in the timeframes required to make the project viable.

Is the processing necessary?

The charity believes that this processing is necessary. Without doing research to find individuals who might be interested in such opportunities (e.g. major donors, high net worth individuals and philanthropists), the charity's ability to fundraise is limited to 'mass' public fundraising (e.g. door drops, advertising) which is less targeted, expensive and unlikely to raise sufficient support for larger projects.

The charity believes the necessity of the processing can be clearly demonstrated through tangible benefits both to the charity such as cost-effective and competitive fundraising and enabling the determination of fundraising strategy/feasibility of key projects and initiatives. The processing can also benefit the major donor community by bringing to their attention projects of interest they may otherwise have not been aware of.

The balancing test

Having established that the charity has a legitimate interest in seeking support for the project, the charity needs to ensure the processing won't override the rights, freedoms & interests of individuals. Care will be taken when completing the balancing test to ensure that the sources of publicly available information that can be utilised are individually and collectively assessed against the reasonable expectations of the individual and to ensure that only relevant personal data is captured from these sources.

The information is being used to ensure individuals are not mistargeted or inappropriately solicited either due to lack of interest in the project, possible known vulnerabilities or sensitivities, or at significantly higher financial level than they could typically afford. The information is restricted to that necessary to understand their likely interest and is not being used in a way that would be deemed 'unreasonable'.

Such activity will provide positive benefits to the individuals through lower levels of inappropriate contact and increased professionalism in approach, something generally expected by this audience. However, as the charity does not have a pre-existing relationship with the individuals they might not expect this particular charity to be processing their data in this way and it may be seen as an invasion of privacy.

Safeguards

In relying upon legitimate interests, safeguards should be put in place to minimise data collection, providing guidance to staff undertaking this activity, particularly around their use of publicly available sources. These safeguards should include

- screening the personal data generated through these sources against a suppression file of those who have opted-out of the charity's direct marketing in the past
- identify strict retention periods
- ensure the individual is provided with a privacy notice at the most appropriate time (usually at the first point of contact), to make them aware that their data has been processed under legitimate interest and give them a clear opportunity to object to further processing.

(D) MEMBERSHIP POSTAL COMMUNICATIONS

A professional association and trade body communicates with its existing members via post for the purposes of direct marketing. These monthly communications include a membership magazine, a member newsletter and the promotion of events/training which support the member, as they are considered professionally relevant, or align with the membership body's objectives.

The membership body has for many years clearly defined these objectives via a mission statement on its website as well as at any joining/on-boarding opportunity for prospective members.

Is this a legitimate interest?

The membership organisation has a legitimate interest in postal marketing communications to existing paying members, who would reasonably expect to receive such communications, in so long as that marketing is related to the membership organisation's mission, values, and objectives. The content is always professionally or socially relevant subject matter and as a result, should result in a positive benefit to the member, forming a key element of the value exchange.

Is the processing necessary?

Members expect to receive marketing such as this as a part of joining the organisation and throughout the member life- cycle, which may last a lifetime. They would not expect to have to separately provide opt-in consent, or to be contacted in order for them to provide this consent.

The demographics of the organisation mean a significant proportion of members joined in the distant past and were never invited to opt-out initially when joining. A larger proportion have signed up via a Fair Processing Notice and offered an opt-out of marketing. Any permission enhancing campaign seeking opt-in consent would likely result in a low response rate, particularly via email, and run the risk of cutting of a proportion of the membership who are time resource poor, or less likely to engage digitally.

The balancing test

A member's focus group was formed to ascertain whether members would reasonably expect such communications. The group were questioned as to whether they would find such communications intrusive, or a key part of the value exchange between paying member and membership organisation. Results were unilaterally positive for the latter assumption.

The membership body has assessed the risk of processing this data via a Data Protection Impact Assessment and has ensured that its processors, including its outsourced mail house have appropriate technical and organisational measures in place; coupled with a suitably robust data processing agreement.

To support the first principle of GDPR, namely lawful and transparent processing; the membership organisation will send a postal update to all existing members who have not previously opted-out of marketing communications. The communication will inform members as to their rights under GDPR and explain that the organisation intends to rely on legitimate Interests as the lawful basis for postal communications, whilst certain digital communications require their opt-in consent. A summary of the legitimate interests' decision will be included in the mailing whilst the organisation's privacy notice will be sign-posted. This sets out the balancing test in more detail and is clear as to the member's right to object.

Safeguards

A clear mechanism for opting out of such processing is provided via a dedicated email address, phone number and postal address. Other relevant safeguards are also in place.

Examples of where legitimate interests may apply

Please note: This broad non-exhaustive list of examples is intended to give an illustration of scenarios in which organisations may consider the use of this lawful basis for processing personal data. All of these examples would be subject to the organisation conducting a LIA to evaluate their own specific circumstances.

1 – FRAUD PREVENTION

An insurance company wants to process personal data as part of its business-critical anti-fraud measures. This is clearly in the company's interests and can also be seen as benefiting customers as the cost of fraud is one of the factors which can push insurance premiums up for all.

2 – RISK ASSESSMENT

Insurance companies need to risk-assess potential customers to determine which products or services the company can offer and the terms of those services. They also need claims information to prevent and detect fraud. They have competition law requirements that limit industry data sharing. Therefore, providers of information services to the insurance industry have set up contributory databases, allowing insurers to contribute data on their own customers and benefit from information on potential new customers held by their competitors. Such an industry database also allows insurers to gather relevant information from across the industry to assess and resolve claims more efficiently, and to prevent and detect fraud.

3 – DUE DILIGENCE

In addition to carrying out statutory requirements, companies may wish to conduct further and necessary corporate due diligence on customers, potential customers and business partners. Providers of diligence information can assist companies with their obligations by making it quick and easy to obtain all the relevant information in one place. This could include, for example, consolidating all the official watch-lists, sanction lists and 'do-not-do-business-with' lists published by governments and other official bodies globally. They also provide keyword searches of industry and reputable publications to determine if companies and individuals have been involved in or convicted of relevant offences, such as fraud, bribery and corruption.

4 – ETHICAL PURPOSES

A refugee charity for ethical and humanitarian reasons processes personal data of individuals located in the EU, for the purposes of assessment and allocation. This is in the interests of both the refugee and the charity.

5 – INDIVIDUAL RIGHTS

A business needs to retain minimal personal data on an individual who has exercised their right to erasure/to be forgotten. They will need to keep basic data to identify that individual and retain it solely for suppression purposes to prevent further unwanted processing. This activity would be in the mutual interests of the individual who wishes their privacy rights to be upheld and the business which is required to fulfil this right.

6 – NETWORK SECURITY

A company monitors access to customer accounts containing personal data to detect and prevent unauthorised access. The company regards this as essential processing activity to protect its customers and employees.

7 – MARKETING SUPPRESSION

A publishing company needs to hold personal data about an individual on its marketing suppression file to make sure there is a record of their objection to direct marketing. The company will hold a minimised record to uphold this request.

8 – MARKETING ANALYICS AND PERSONALISATION

A travel company relies on consent for its marketing communications but relies on legitimate interests to perform marketing analysis to inform its marketing strategy, and to personalise messages to its customers for mutual benefit.

9 – PROFILING

In carrying out its risk modelling an insurance company captures and uses a range of personal data in order to assess factors affecting those risks, for example age, location and claims history.

10 – PROFILING USING THIRD PARTY DATA

A multi-channel retailer wishes to append information sourced from a third party to its database for the purpose of profiling its existing customer base and improving the relevance of postal communications to its customers. This is necessary for the retailer to make sure its marketing strategy is effective. The retailer ensures the profiling does lead to bias or discrimination. The retailer informs its customer of this activity via a suitably transparent privacy notice. When the data is initially captured by the third party, individuals are provided with a clear opportunity to opt-out of their data being shared and are provided with information about recipients in a transparent privacy notice. The third party who collected the data makes it easy for individuals to request their data is no longer used for this purpose. These requests are flowed down to the multi-channel retailer who is contractually bound to honour any request to stop such processing.

11 – EVIDENTIAL PURPOSES

A hotel logs customer entries and exits to their hotel rooms, as well as employee access to the customers' rooms by using key card data. This information is used to manage disputes with guests, any investigations into staff misconduct and separately to administer guest stays and improve customer experience. The data is limited and normally only retained for 31 days, then deleted.

12 – EMPLOYEE RELATIONS

A financial services company processes an employee's contact details to arrange business travel, and ensure the employee receives benefits and personal development opportunities.

13 – HUMAN RESOURCES RECORDS

A distribution company processes employee data to provide optional staff benefits e.g. health plan and gym membership.

14 – DIRECT MARKETING

A charity sends a postal mailshot out to existing supporters providing an update on its activities and details of upcoming events.

Note: GDPR Recital 47 states: *'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest' and also states 'An organisation may wish to rely upon legitimate interests where consent is not viable or not preferred.'* This confirms direct marketing is legitimate, but doesn't cover the balancing test. Most Data Protection Authorities would still expect the organisation to conduct an LIA.

15 – ANALYTICS AND MONITORING

A retailer requests its call centre operators to use a software solution which uses both personal and non-personal data to identify recurring problems and analyse the patterns of customer and staff behaviour. The solution includes capturing and processing calls and is used to enable the call centre to ensure optimum staff performance and to serve customers better. A notification is included on the IVR message at the beginning of all calls.

16 – ARTIFICIAL INTELLIGENCE

An employer uses AI-driven psychometrics tests as part of its recruitment process. This activity is considered necessary to ensure candidates have the relevant skills, understanding and abilities for the role, whilst reducing the burden on the recruiting manager's time. Safeguards should be in place to minimise data collection and ensure its use is proportionate. Job applicants must be notified of any use of profiling and/or automated decision making. A procedure needs to be in place to handle any objections which may be received. A DPIA needs to be carried out for this activity and perhaps a separate AI Risk Assessment too.

17 – NON-REPETITIVE INTERNATIONAL TRANSFERS

A charity transfers the personal details of refugees in the EU to a third country which has a programme of refugee settlement.

Note: International transfers which can be qualified as not repetitive and that only concern a limited number of individuals, are recognised as possible for the purposes of the compelling legitimate interests pursued by a controller (when those interests are not overridden by the interests or rights and freedoms of the individual and when the controller has assessed all the circumstances surrounding the data transfer).

18 – PERSONAL DATA USE IN AN ACQUISITION

A publisher acquires circulation data in a business acquisition of several magazines and wishes to use the data for similar and compatible purposes to those for which it was originally acquired.

19 – UPDATING CUSTOMER DETAILS AND PREFERENCES

A retail company uses an external service provider to verify the accuracy of customer data and create a better understanding of its customers. The company would need to carefully consider how it was conducting this and what the reasonable expectations of its customers would be.

20 – LOGISTICS

A supermarket chain needs to establish where best to locate its distribution points and how to allocate products within warehouses. The business needs to process minimal customer data to predict future demand. Additional data is externally sourced to enrich the customer records and inform these decisions.

21 – ROAD TRAFFIC DATA

Real-time road traffic data is collected and minimised for modern traffic routing services in both the private and public sectors, allowing greatly improved efficiency in the management of traffic in densely populated areas. It enables car navigation systems and is used by individuals, the public sector, and commercial fleets. The data used for this is emitted by mobile phones, connected cars and other end-user devices.

22 – SEASONAL HEALTH TRENDS

Personal data is processed for scientific statistical research purposes. Minimal data relating to individuals searching the internet about flu is aggregated to produce outputs that can be highly useful to public authorities and beneficial to society at large, helping to better understand the spread of diseases like flu.

23 – HR BACKGROUND CHECKS

An organisation wishes to process personal data to undertake background vetting of people it has given job offers to. This will include asking for references from previous employers. The organisation makes sure potential employees are fully aware this will take place and no sensitive data will be used as part of this process. It should be noted certain other background checks may rely on the consent of the individual.

24 – CHARITY MAILING TO PREVIOUS DONORS

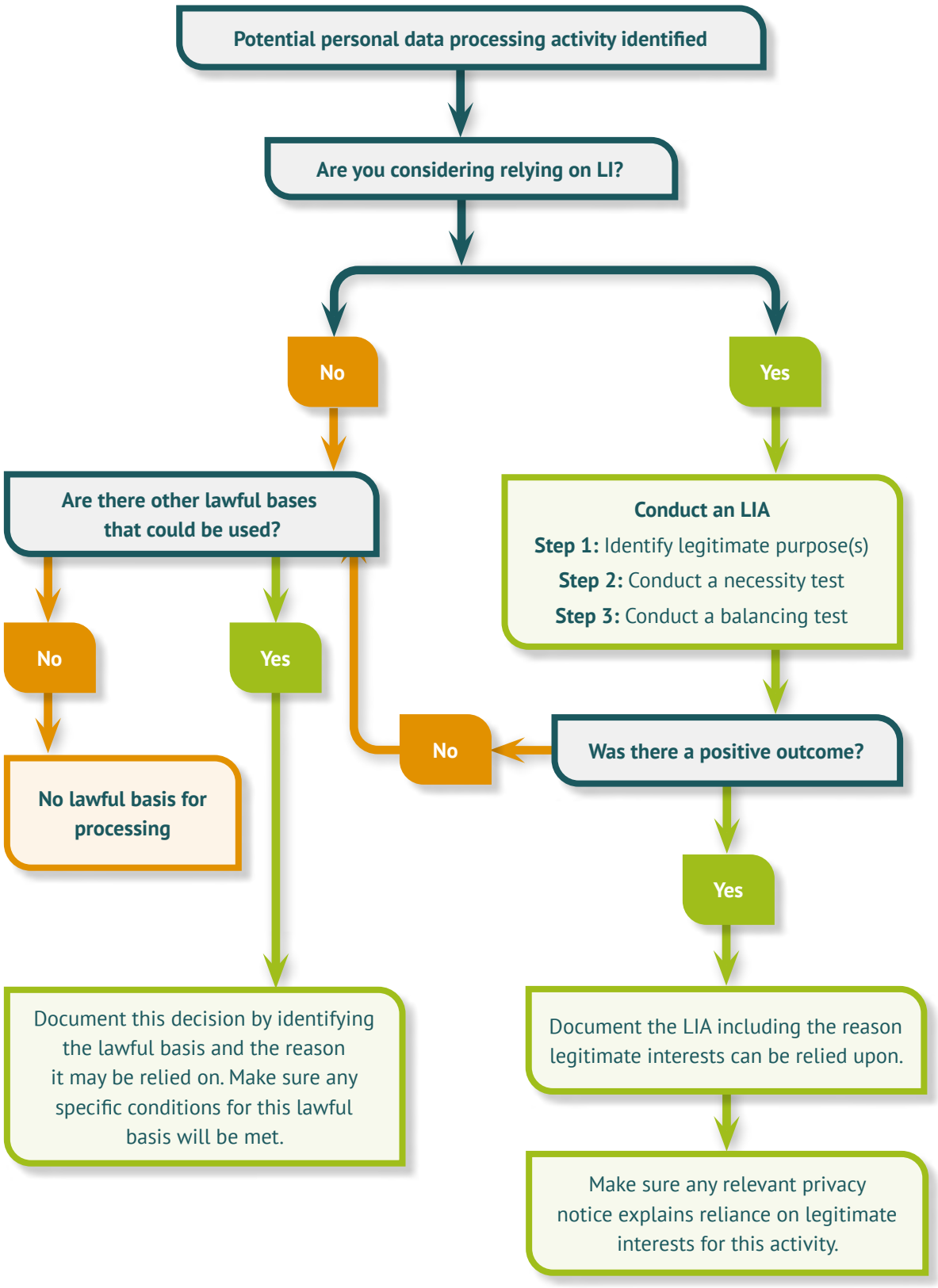
To raise necessary funds for its cause, a charity would like to send information by postal mail about its work, including its latest fundraising appeal to individuals who donated in the past year. The charity believes this activity to be proportionate and within the donors' reasonable expectations. The charity has provided clear information in their fair processing notices and privacy notice that they would like to send them direct marketing in future, given a clear opportunity to object and exclude all customers who have opted-out.

25 – MONITORING TO ENSURE ACCEPTABLE USE OF IT SYSTEMS

A company collects data from its employees' computers and mobile devices as part of its data loss prevention (DLP) strategy. This is carried out to protect the data it holds by preventing employees from uploading sensitive or critical business information to physical devices or external cloud storage.

The process operates by implementing alerts regarding specific activities. For example, if a salesperson begins to print out or download a copy of all their sales contacts this raises a 'red flag' in the IT department that this person may be doing this for unauthorised purposes. The company provides an Acceptable Use Policy to its employees stating why this monitoring is undertaken using company devices to protect the company's commercial interests and trade secrets.

Legitimate interests process flow



Appendix A: Related GDPR Articles and Recitals

Article 6(1) (f) "Lawfulness of processing"	Processing shall be lawful only if and to the extent that at least one of the following applies: **a.** the data subject has given consent to the processing of his or her personal data for one or more specific purposes; **b.** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; **c.** processing is necessary for compliance with a legal obligation to which the controller is subject; **d.** processing is necessary in order to protect the vital interests of the data subject or of another natural person; **e.** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; **f.** **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.**
Article 13(1) (d) "Information to be provided where Personal data are collected from the data subject"	**1.** Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: **a.** the identity and the contact details of the controller and, where applicable, of the controller's representative; **b.** the contact details of the data protection officer, where applicable; **c.** the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; **d.** **where the processing is based on point (f) of *Article 6(1)*, the legitimate interests pursued by the controller or by a third party;** **e.** the recipients or categories of recipients of the personal data, if any; **f.** where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of *Article 49(1)*, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Article 14(2) (b) **"Information to be provided where personal data have not been obtained from the data subject"**	In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; b. **where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;** c. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to Data Portability; d. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; e. the right to lodge a complaint with a supervisory authority; f. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; g. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
Article 21 **"Right to Object"**	2. **The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.** 3. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. 4. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. 5. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. 6. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications. 7. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22(2) (b) **"Automated individual decision- making, including profiling"**	1. The data subject shall have the right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision: a. is necessary for entering into, or performance of, a contract between the data subject and a data controller; b. **is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or** c. is based on the data subject's explicit consent.
Article 49(1) **"Derogations for specific situations"**	In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; d. the transfer is necessary for important reasons of public interest; e. the transfer is necessary for the establishment, exercise or defence of legal claims; f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; g. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. **The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.**

Recital 47 **Overriding Legitimate Interest**	The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.
Recital 48 **Overriding Legitimate Interest Within Group Of Undertakings**	Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' Personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

Recital 49 **Network and Information Security as Overriding Legitimate Interest**	The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.
Recital 50 **Further Processing of Personal Data**	The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations. Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

Recital 68 **Right of Data Portability**	To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable Data Portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right have the data transmitted directly from one controller to another.

DATA PROTECTION NETWORK

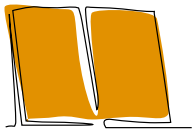
About DPN

Founded in 2014 we regularly publish news, insight and guides. Our experienced team work across a range of sectors providing tailored data protection training, data protection gap analysis reviews and helpdesk support.

Get in touch

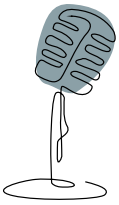
Consultancy

No-nonsense, practical data protection cunsultancy from our experienced team



Articles

News, insight and how-to-guides to support your day-to-day protection work



Events

Expert speakers share knowledge and tips on a range of privacy topics

Training

Down-to-earth data protection training workshops focused on developing your team's skills

Simon Blanchard
simon@dpnetwork.org.uk

Philippa Donn
phil@dpnetwork.org.uk

Get DPN updates direct to your inbox
Sign up here

www.dpnetwork.org.uk