



BRISTOWS



ISBA

iab UK

Institute of Fundraising

IPA
Incorporated
by Royal Charter

Balfour Beatty

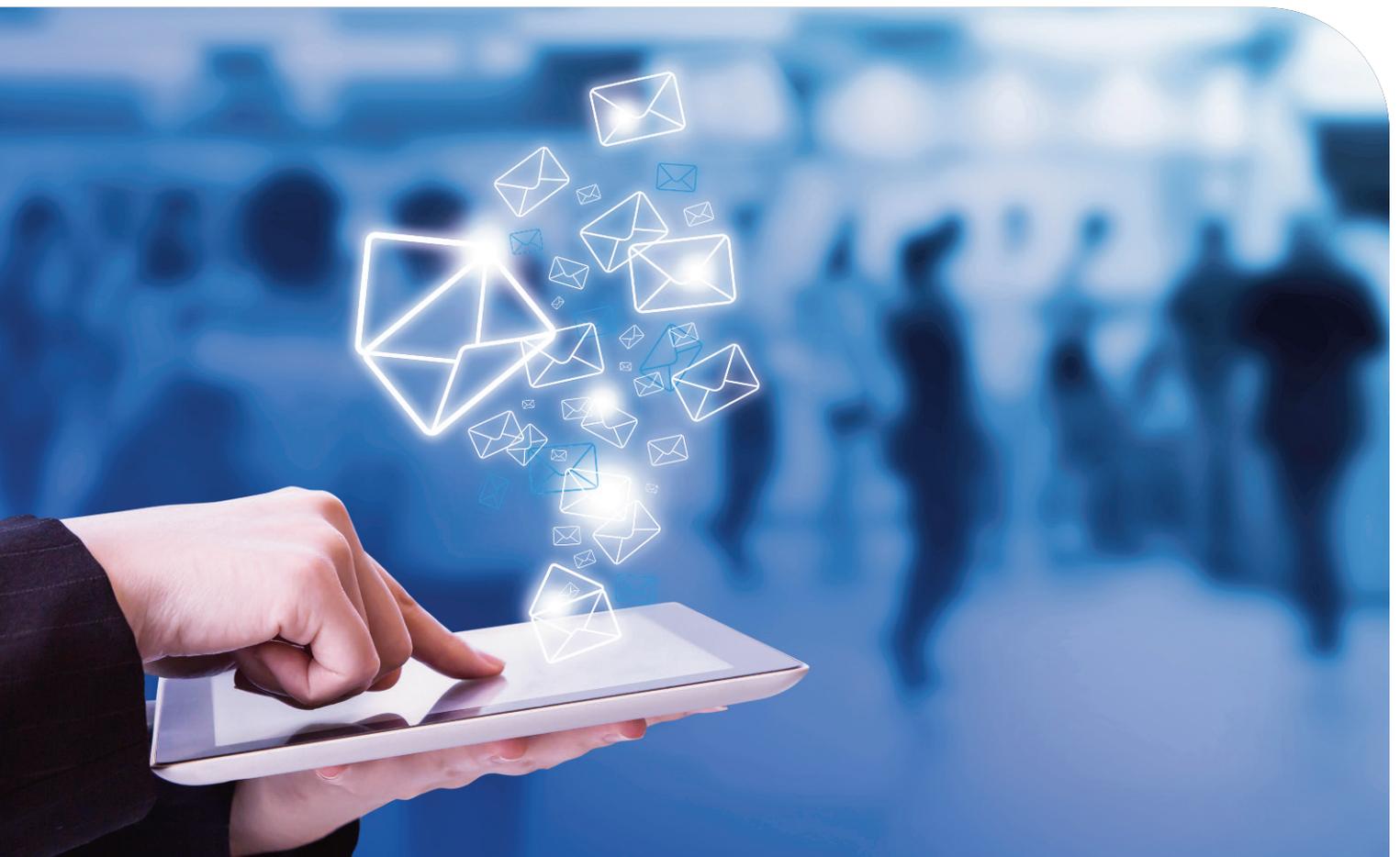
drifrock

EPSILON

HARTE
HANKS

MEMBER360

Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation



For commercial, not-for-profit organisations, and for individuals

06.04 2018 Version 2.0

Copyright of Data Protection Network. All rights reserved. 2018 ©

About this Guidance

An initiative of the Data Protection Network (www.dpnetwork.org.uk), this Guidance has been made possible by contributions from Bristows LLP, the Direct Marketing Association, ISBA, the IAB, the Institute of Fundraising, the IPA, Balfour Beatty, Drifrock, Epsilon, Harte Hanks, Member 360 and other representatives of some of the largest companies and institutions in the UK.

This Guidance has been welcomed by the Information Commissioner's Office and the Data Protection Commissioner of Ireland and should be read in conjunction with official guidance from these and other European Regulators.

The purpose of version 2.0 of this Guidance is to provide several case studies of where Legitimate Interests might apply and to provide more short examples. We have also enhanced the Legitimate Interests Assessment (LIA) template (Appendix B) and provided a sample of a completed LIA (Appendix C). We have not made any significant changes to the body of the Guidance itself.

The information provided in this Guidance represents the views of the Data Protection Network's Legitimate Interests Working Group. It does not constitute legal advice and cannot be construed as offering comprehensive guidance to the General Data Protection Regulation (Regulation (EU) 2016/679) or other statutory measures referred to in the document.

Copyright of Data Protection Network. All rights reserved. 2018 ©

Foreword

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) aims to harmonise data protection legislation across EU member states, enhancing privacy rights for individuals. It applies to organisations processing Personal Data which have an establishment within the EU and also those organisations which operate outside the EU but offer goods or services to, or monitor the behaviour of, individuals in the EU. The GDPR is applicable from 25 May 2018.

The GDPR sets out six lawful grounds for processing, one of which is processing under the Legitimate Interests of a Controller, including those of a Controller to which the Personal Data may be disclosed, or of a Third Party.

Under 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.'

As well as providing the right for individuals to object to the processing of Personal Data based on Legitimate Interests, the GDPR sets out strict criteria for organisations that seek to rely on Legitimate Interests. These include establishing that the processing is necessary and that a balancing test has been conducted. The GDPR does not specifically list all circumstances where Legitimate Interests might be relied upon.

Purpose

The purpose of this Guidance is to help commercial and not-for-profit organisations to understand the circumstances in

which Legitimate Interests may apply. This Guidance does not consider any other grounds for processing under the GDPR. Although Article 6 restricts the ability of public authorities to rely on Legitimate Interests, 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 Guidance provides practical advice on assessing whether the processing might be considered "necessary" and meeting the crucial **Balance of Interests Condition**, whereby Controllers need to ensure their interests, or those of a Third Party, are not overridden by the interests or fundamental rights and freedoms of individuals.

This Guidance considers a wide spectrum of processing activities, both core and elective, which may be covered by Legitimate Interests. Our intention is to provide a framework that Controllers can apply to their own specific circumstances.

This Guidance underlines the importance of conducting and documenting **Legitimate Interests Assessments (LIAs)** wherever a Controller seeks to rely on Legitimate Interests, even where the balance of interests is clearly in favour of the Controller. The ICO has expressed full support for the central concept of a Legitimate Interests Assessment (LIA), and documenting this on a template. Such an assessment will certainly assist organisations in meeting their accountability and transparency requirements and ensure that individuals' interests are put front and centre under the GDPR regime.

This Guidance also aims to offer clarity for individuals on why processing under Legitimate Interests may be advantageous to them, as well as to Controllers.

In order to meet the **GDPR transparency requirements**, this Guidance offers advice on how best to articulate and inform individuals, using fair processing notices, about the circumstances in which their Personal Data may be processed under Legitimate Interests. If this Guidance is widely adopted, it will provide a consistent approach for the benefit of both organisations and individuals.

Introduction from the Chairman of the Data Protection Network

I am delighted that the Data Protection Network and other collaborators have been able to publish this Guidance. I appreciate the work of all involved and the Information Commissioner's Office for valuable scrutiny and comment. We are pleased to have benefitted from the support of Regulators and contributors in making this a practical document.

Robert Bond, Partner and Notary Public for Bristows LLP

Overview

This Guidance is a practical tool to help commercial and not-for-profit organisations assess whether or not they can rely on Legitimate Interests as a Lawful Basis for processing Personal Data under the GDPR.

An essential part of the concept of Legitimate Interests is the balance between the interests of the Controller and the rights and freedoms of the individual:

*'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.'*¹

It is important to note that this Guidance reflects the law as set out under the GDPR and will be subject to the finalisation of the proposed Regulation on Privacy and Electronic Communications. The final text of this proposed Regulation has yet to be published.

¹GDPR Article 6(1)(f)

Contents of this Guidance

Understanding what Legitimate Interests are

Key definitions	06
The Lawful Basis for processing under the GDPR	07
Individuals' rights under the GDPR & the implications of using Legitimate Interests	08

Identifying areas of processing where Legitimate Interests may apply

How Legitimate Interests might apply	09
Case studies & examples of where Legitimate Interests may apply	10

The Legitimate Interests Assessment (LIA) - the 3 stage test

Identifying a Legitimate Interest	17
The 'necessity test'	17
The 'balancing test'	17

Transparency and the consumer

How to communicate the use of Legitimate Interests effectively and transparently to individuals	19
---	----

Appendices:

Appendix A – Legitimate Interest Process Flow for selecting Lawful Basis for processing	22
Appendix B – Legitimate Interests Assessment Template	23
Appendix C - Legitimate Interests Assessment Example	29
Appendix D – The GDPR articles and recitals relating to Legitimate Interests	35
Appendix E – Glossary of terms	41

Understanding what Legitimate Interests are

Key definitions

When considering Legitimate Interests as a ground for processing it is important to take note of the specific wording in Article 6 (1)(f):

*'Processing will be lawful if it is **necessary** for the **purposes** of the **legitimate interests** pursued by the controller or 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.'*

In practice, Legitimate Interests can only be relied upon as a Lawful Basis of processing to the extent that such activity is '**necessary**' (for the purpose of the Controller's or a Third Party's Legitimate Interests).

Whilst evaluating whether processing is 'necessary', Controllers also need to take into account whether on balance their Legitimate Interests are outweighed by the rights and freedoms of the individual and that the processing would not cause unwarranted harm. This is called a 'balancing test'.

'**Purpose**' is the specific reason why the data is being processed.

An '**interest**' is the broad stake a Controller may have in the processing, or the benefit that the Controller derives, or which society might derive, from the processing. It must be real and not too vague. For example, many businesses want to make a profit. This does not mean that the broad objective is a Legitimate Interest in and of itself.

An '**interest**' can be considered as '**legitimate**', as long as the Controller can pursue this interest in a way that complies with data protection and other laws.

Article 6(1)(f) provides protection for individuals by requiring that all their relevant '**interests**' and '**rights and freedoms**' (including but not limited to their privacy rights, such as the European Convention on Human Rights) should be taken into account and weighed against the interests of the Controller.

Some interests are likely to be legitimate because they are 'strictly necessary' for corporate governance or related legal compliance issues, particularly where there is no legal obligation to comply with, but the processing is essential to ensure the Controller meets external or internal governance obligations. Other interests are legitimate because they are a routine part of the activities of the Controller but other lawful reasons for processing are not practical or are not available. Regardless of the importance of the processing activity to the Controller, an assessment must be made to ensure the processing meets the threshold required to rely on Legitimate Interests as a Lawful Basis.

Although this is not a term used in the GDPR, this Guidance uses the term Legitimate Interests Assessment or LIA to mean:

1. The assessment of whether a Legitimate Interest exists;
2. The establishment of the necessity of processing; and
3. The performance of a balancing test to decide if a particular processing operation can rely on the Legitimate Interests provision in the GDPR as a Lawful Basis for processing that Personal Data

This is the same principle found in the ICO and Article 29 Working Party guidance and opinions.

(Also see Glossary of Terms – [Appendix E](#))

The Lawful Basis for processing under the GDPR

Controllers must have a Lawful Basis for processing Personal Data, under the GDPR and these are set out in Article 6.1 as follows:

- a) **CONSENT** – the individual has given their Consent to the processing of their Personal Data.
- b) **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 pre-contractual steps at the request of the individual.
- c) **LEGAL OBLIGATION** – processing of Personal Data is necessary for compliance with a legal obligation to which the Controller is subject.
- d) **VITAL INTERESTS** – processing of Personal Data is necessary to protect the vital interest of the individual or of another individual.
- e) **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.
- f) **LEGITIMATE INTERESTS** – processing is necessary under the Legitimate Interests of the Controller or Third Party, unless these interests are overridden by the individual's interests or fundamental rights.

Is consent the most important Lawful Basis for processing?

It is important to note that there is no hierarchy of Lawful Bases for processing Personal Data: all are equally valid. Controllers may choose a different Lawful Basis for different processing activities. The most appropriate Lawful Basis will depend on the Personal Data being processed and the purposes for processing.

Legitimate Interests may be considered where:

- another Lawful Basis is not available due to the nature and/or scope of the proposed processing; or
- where there are a number of Lawful Bases that could be used but Legitimate Interests is the most appropriate

Telling Individuals about the Lawful Basis of Processing

Under the GDPR, Controllers must be clear and transparent about which Lawful Basis they are using as;

- i) different Lawful Bases give rise to different obligations under the GDPR;
- and
- ii) Controllers should record which Lawful Basis they are choosing for their different processing activities and their reasons for choosing that Lawful Basis.

It is also important to note that, in addition to satisfying one of the Lawful Bases for processing Personal Data, Controllers must comply with the data protection principles² in the GDPR. Under the transparency provisions in the GDPR, Controllers must set out what their Legitimate Interests are when they rely on this as their Lawful Basis for processing.

Processing for secondary purposes – Recital 50 & Article 6(4)

If the purpose of the processing changes the Controller would need to evaluate and document whether the new purpose is compatible, taking into account;

- (a) any link between the original purpose and the intended future processing
- (b) the context in which the Personal Data was collected; specifically, the relationship between the Controller and the individual
- (c) the nature of the Personal Data
- (d) the possible consequences of the change of purpose on individuals
- (e) the existence of appropriate safeguards, e.g. encryption or pseudonymisation

² GDPR Article 5 'Principles relating to processing of Personal Data'

Individuals' rights under the GDPR and the implications of using Legitimate Interests

When considering which Lawful Basis is most appropriate to rely on for the processing of Personal Data, Controllers should take into consideration the privacy rights of individuals under each Lawful Basis of processing. It is important to note these rights may differ depending on which Lawful Basis a Controller may choose to rely.

Example – Consent Vs Legitimate Interests

Different rules apply depending on whether the Controller is relying on Legitimate Interests or another basis for processing, such as Consent.

For example, if a Controller relies on Legitimate Interests for its profiling activities the individual has a right to object to profiling under Article 21. However, if the Controller uses Consent for its profiling activities the individual does not have this right (although they can withdraw their Consent at any time).

Therefore, on balance, a Controller may wish to rely on its Legitimate Interests, as it has the opportunity to defend this decision, whereas when Consent is withdrawn, the processing must cease immediately.

As always, the Controller would be advised to check that it is able to rely on Legitimate Interests by conducting a Legitimate Interests Assessment (LIA).

Overall the GDPR provides the following rights for individuals, many of which apply whatever the basis of processing, although there are some exceptions:

1. The right to be informed how Personal Data is processed
2. The right of access to their Personal Data
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Legitimate Interests and the obligation to inform individuals

Controllers need to be aware that if they use Legitimate Interests rather than other Lawful Bases, individuals must

be told about those Legitimate Interests and there is also an obligation to tell individuals about their right to object.

Right to erasure and Legitimate Interests

The 'right to erasure' is not an automatic right for individuals where processing is based on Legitimate Interests. However, this would be the case if Consent was the Lawful Basis³. That said, even where the Controller relies on Legitimate Interests for the processing, an individual will still have the right to object to the processing of their Personal Data⁴. The right to erasure would then apply if the Controller could not justify the legitimacy of the processing. Additionally, the right still applies when relying on Legitimate Interests where the Personal Data is no longer required for the purpose it was originally collected, or where the processing is found to be unlawful.

Legitimate Interests and the right to object

When processing is based on Legitimate Interests, the Controller must inform individuals of their right to object to such processing. This can be highlighted to an individual at the point of data collection (when explaining what Legitimate Interests means) and in the section of a Privacy Notice that deals with individuals' rights.

In some cases, such as direct marketing, an objection from an individual will be sufficient to mean the Controller's Legitimate Interests are overridden. In this situation the Controller must uphold the individual's right to object and exclude them from such processing. However in other cases, such as fraud prevention or network and information systems security, an objection may not be enough to be sufficient to override the Controller's Legitimate Interests.

Controllers will also need to consider what tools will be required to allow individuals to object. These are likely to vary depending on the processing conducted. For example, an objection to processing for direct marketing may be able to be requested and actioned automatically by the individual (through an unsubscribe link or online preference centre), whereas an objection to other forms of processing may need to be further considered and actioned by the Controller. Controllers should consider the impact of any individual's objection when conducting the balancing exercise to identify how an objection will be handled in advance.

Right of data portability and Legitimate Interests

The right of data portability does not extend to Personal Data processed on the basis of Legitimate Interests. However, you should refer to official guidance regarding the scope of the right to portability, particularly in relation to "observed" data."

³GDPR Recital 68 ⁴GDPR Article 21

Identifying areas of processing where Legitimate Interests may apply

How Legitimate Interests might apply

3 Stage Test

A Controller may rely upon its Legitimate Interests subject to identifying a Legitimate Interest, establishing that the processing is 'necessary' and conducting a balancing test. The Legitimate Interest can be one of the Controller or of a Third Party to whom the data may be disclosed, as long as the 3 stage test is passed.

Direct vs Indirect Relationships

The context of the relationship between the individual and a Controller is a key element in understanding the legitimacy of the processing activity. It does not necessarily matter if there is a direct or indirect relationship between the individual and the Controller to have a Legitimate Interest, but it will be a factor to consider in a balancing test. The nature of the relationship should be weighed against the necessity of the processing and the impact on the individual.

Disclosure to Third 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 Party⁵ would have to be taken into consideration.

What examples does the GDPR provide?

Recitals 47 to 50 in the GDPR give some examples of when a Controller may have a Legitimate Interest which would need to be confirmed by an LIA:

1) DIRECT MARKETING - processing for direct marketing purposes under Legitimate Interests is specifically mentioned in the last sentence of Recital 47.

2) REASONABLE EXPECTATIONS - the fact that individuals have a reasonable expectation that the Controller will process their Personal Data, will help the make the case for Legitimate Interests to apply when conducting the balancing test.

3) RELEVANT & APPROPRIATE RELATIONSHIP - where there is a relevant and appropriate relationship between the individual and the Controller in situations where the individual is a client or in the service of the organisation. However, this does not mean that 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 that 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 that 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, the rules on transferring Personal Data to a country outside the European Economic Area (EEA) must be complied with if this is 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 authorised users' access to a Controller's computer network for the purpose of preventing cyber-attacks.

⁵GDPR Article 14

Case Studies and Examples of where Legitimate Interests may apply

There will undoubtedly be a wide range of processing activities for which a Controller may wish to consider using Legitimate Interests as the Lawful Basis for processing Personal Data, subject to an LIA. This may be processing that is clearly for the individual's benefit, for the mutual benefit of both the individual and the Controller (and Third Party) for organisational activities, or where the Controller 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. (See Legitimate Interests Assessments)

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 of their Legitimate Interests.

(A) TELEMATICS

What is Telematics?

Telematics means the transmission of data about remote devices or vehicles over a network. Telematics are used for a variety of purposes, such as monitoring vehicle performance, driving behaviour and road safety. Telematics are often used to by insurance companies to validate claims by using sensors placed on customer vehicles to detect speed and direction of impact at the time of an incident and by others to manage the availability of resources, such as a fleet of lorries or taxis etc.

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 businesses to ensure that vehicles being operated by their employees are being operated 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 Controller'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 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 policies 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 where 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 if 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 machines. They control 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 machine is being used outside business hours (if appropriate).

Note: for this Case Study we have provided an example LIA in [Appendix C](#)



(B) CHARITY PROSPECTING

A charity has taken over an old cinema and are 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; and 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 privacy rights 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. To identify strict retention periods and to 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.

C) 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 sending marketing 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 before the existing Data Protection Act and were never asked 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 off 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 providing they have not previously opt-out of marketing communications.

The communication will inform members as to their new 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 may require their opt-in consent. A summary of the legitimate interests' decision will be included in the mailing whilst the organisation's online Privacy Policy 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.

EXAMPLES OF WHERE LEGITIMATE INTERESTS MAY APPLY

PLEASE NOTE: The broad non-exhaustive list of examples provided below are intended to give an illustration of scenarios in which Controllers may consider the use of this condition for processing Personal Data. All of these examples would be subject to the Controller conducting an LIA to evaluate their own specific circumstances. This assessment should take into account the following:

- The relationship between the Controller and the individual
- The sensitivity of the personal data involved and whether it includes children’s data
- The vulnerability of individuals
- The rights and freedoms of individuals
- The reasonable expectations of the individuals
- Would individuals be likely to object to this use or find it intrusive
- The size of impact the activity could this have on the individual
- Potential safeguards to minimise the impact
- The ease with which individuals could opt-out

Example 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 interests of the Controller but could also be seen as benefiting customers as the cost of fraud is one of the factors that can push up insurance premiums for all.

Example 2 – RISK ASSESSMENT

Insurance companies need to risk assess potential customers to determine what products or services they 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.

Example 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 are able to assist companies with their obligations by making it quick and easy to obtain all their 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. As well as providing 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.

Example 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.

Example 5 – INDIVIDUAL RIGHTS

A business needs to continue processing 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.

Example 6 – NETWORK SECURITY

As specified in its IT governance policies, a mail order company monitors access to accounts containing Personal Data by named users within the organisation to prevent theft of data by employees. The mail order company regards this as essential processing activity to protect its customers.

Example 7 – SUPPRESSION

A publishing company needs to hold Personal Data about an individual on a suppression file to ensure there is a record of their objection to direct marketing. The company will hold a minimised amount of Personal Data in order to uphold this request. Alternatively, the company could rely on Article 6(1) (c) – necessary for compliance with legal obligation, which would mean that an LIA would not be required.

Example 8 – PERSONALISATION

A travel company relies on Consent for its marketing communications, but may rely on legitimate interests to justify analytics to inform its marketing strategy and to enable it to enhance and personalise the “consumer experience” it offers its customers.

Example 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.

CONDUCT LIA!

Necessary?

Reasonable?

Impact?

Intrusive?

Balanced?

Opt-out?

Documented?

**CONDUCT
LIA!**

Necessary?

Reasonable?

Impact?

Intrusive?

Balanced?

Opt-out?

Documented?

Example 10 – 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.

Example 11 – EMPLOYEE RELATIONS

A financial services company processes an employee's contact details in order to arrange business travel, and ensure the employee receives benefits and training.

Example 12 – HUMAN RESOURCES RECORDS

A distribution company processes the Personal Data of its employees in order to provide optional staff benefits e.g. health plan and gym membership.

Example 13 – DIRECT MARKETING

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

Note: The GDPR says, 'the processing of Personal Data for direct marketing purposes may be regarded as carried out for a legitimate interest.' An organisation may wish to rely upon Legitimate Interests where Consent is not viable or not preferred and the Balance of Interests condition can be met. The GDPR states "may be regarded as...", so organisations will still need to ensure they can establish necessity and balance their interests with the interests of those receiving the direct marketing communications.

Example 14 - MONITORING

A retail company requests its call centre operators to use a software solution which uses big data to identify recurring problems and analyse the patterns of behaviour of customers and staff. This solution includes capturing and processing the 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.

Example 15 – ARTIFICIAL INTELLIGENCE

A customer service department, is putting in place algorithms that help to manage customer service requests. The system would use artificial intelligence methods to route customer contacts to the most appropriate part of the organisation. These routes could link individuals to specific agents who can handle specific requests, but in addition the algorithm might ask a series of questions and provide appropriate answers without the need for human intervention.

Example 16 – WEB ANALYTICS

A social media platform uses diagnostic analytics to assess the number of visitors, posts, page views, reviews and followers in order to optimise future marketing campaigns.

Example 17 – HOSTING DATA IN THE CLOUD

An airline adopts cloud-based services for hosting the data of EEA citizens. This will include where cloud based data services are used to archive data from the live processing environment.

Example 18 – LIMITED 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).

Example 19 – PERSONAL DATA TRANSFERRED IN AN ACQUISITION

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

Example 20 – POSTAL MARKETING FROM THIRD PARTIES

A catalogue company adds details to its online order forms which indicate that it shares data with other cataloguers. The purchaser can opt-out of this sharing and the cataloguers are listed in the Privacy Statement.

Example 21 – 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.

Example 22 – 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 customer data in order to predict future demand. Additional data is externally sourced to enrich the customer records and inform these decisions.

Example 23 - ROAD TRAFFIC DATA

Real-time road traffic data is collected 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.

Example 24 – SEASONAL HEALTH TRENDS

Personal Data is processed for scientific statistical research purposes. A minimal amount of data relating to when individuals searched 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 try and understand the spread of diseases like flu.

Example 25 - 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 ensures potential employees are fully aware that this processing of their personal data will take place and no sensitive data will be used as part of this process.

Example 26 – CHARITY MAILING TO PREVIOUS DONNORS

In order to raise necessary funds for its cause, a charity would like to send information by 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 statement that they would like to send them direct marketing in future, gave a clear opportunity to object and undertake to exclude all customers who have opted-out.

Example 27 – PROFILING USING THIRD PARTY DATA

A multi-channel retailer wishes to append information it has sourced from a third party to its database for the purpose of profiling its existing customer base to ensure postal communications to its customers are more relevant. This is necessary for the retailer to ensure its marketing strategy is effective. The retailer ensures this profiling does not contain prejudicial elements and that the personal data that it sources from the third party is accurate and up to date. 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 subsequently

request that their data is no longer used for this profiling purpose for more relevant postal mailing. These requests are flowed down to the multi-channel retailer who is contractually bound to honour any request to stop such processing.

Example 28 – PROFILING FOR SOCIAL MEDIA TARGETING

As part of a multi-media marketing campaign, a furniture retailer wishes to use a social media platform to target advertising to existing customers whilst they engage with social media. They also wish to use an algorithm provided by the social media provider to better target its advertising to 'lookalikes' - i.e. other individuals who have similar characteristics to that business' own customers. The business uploads the minimum required personal data on its customers to enable the social media targeting, but excludes those who have objected to marketing. Profiling is conducted within the social media platform to enable the targeting, however it is purely for marketing purposes and the business has assessed that it does not result in any legal or similarly significant effects upon those individuals.

Example 29 – AUTOMATED PROCESSING BASED ON CUSTOMER HISTORY

A retailer with a wide product range conducts automated processing which is based on a customer's transactional history, for the purpose of predicting what other products and services they may be interested in. An alert based upon this processing may be presented to one of the company's call handlers when the individual calls in, or a relevant message may be directly to the customer themselves in a self-serve digital journey. Customers are informed about this activity via the Privacy Notice and are given the opportunity to object to this processing. The customer will not be disadvantaged by this process (e.g. they will not be offered selective pricing), in fact they will receive better targeted offers than would have been possible without the processing.

Example 30 - IT SUPPORT

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 uploading sensitive or critical business information to an outside storage service. The process would operate by implementing alerts surrounding specific activities, for example, if a salesperson begins to print out all their sales contacts, this would raise a flag in the IT department that this person may be doing this as they plan to leave the company. The company provides a notice to its employees that it is monitoring their behaviour on company devices to protect the company's commercial interests and trade secrets.

CONDUCT LIA!

Necessary?

Reasonable?

Impact?

Intrusive?

Balanced?

Opt-out?

Documented?

The Legitimate Interests Assessment (LIA) – the “3-stage test”

An essential part of the concept of Legitimate Interests is the balance between the interests of the Controller and the rights and freedoms of the individual:

*‘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.**’⁶*

If a Controller wishes to rely on Legitimate Interests for processing Personal Data it must carry out an appropriate assessment, which we have called a Legitimate Interests Assessment, or LIA. When carrying out an assessment, the Controller must balance its right to process the Personal Data against the individuals’ data protection rights.

In certain circumstances, an LIA may be straightforward. However, it is advisable for the Controller, in order to ensure compliance with Article 5(2) of the GDPR, to maintain a written record that it has carried out an LIA and the reasons why it came to the conclusion that it met the balancing test elements. These LIAs may be disclosed to other Controllers in the event of a sale or acquisition of Personal Data, where Legitimate Interests is the Lawful Basis of processing, as part of the due diligence process. **The Controller to whom Personal Data is disclosed will 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.

By conducting an LIA, the Controller can ensure that the privacy rights of individuals are given due consideration. While the Legitimate Interests of the Controller will often

be aligned with the interests of the individual (e.g. to ensure individuals receive an optimised service from the Controller they are engaged with) sometimes those interests will not be aligned. The Controller must consider if the individual’s rights override the Controller’s interests and if any potential harm that may occur as a result of the processing.

Requirement to carry out an LIA – Balancing Interests against the rights of individuals

Where a Controller wishes to rely on Legitimate Interests as the Lawful Basis for a processing operation, it will need to be able to demonstrate to a Supervisory Authority and/or an individual, if challenged, that it has fully considered the necessity of the purpose of processing against the rights of the individuals and came to a decision that the individual’s rights did not override the interest of the Controller. The decision should be documented and reviewed if the scope of the processing operation changes.

The **LIA template in Appendix B** has been specifically developed to help Controllers carry out this balancing test and document their decisions. However, it can be adapted to suit the sector and industry of the Controller.

Who should carry out an LIA?

The Controller should determine who completes an LIA, who contributes to the evaluation process and who signs it off. Where it is practical to do so, the Controller may wish to create a separation of responsibilities, between the person who signs-off the LIA and those who stand to benefit from the processing. In short, any conflict of interests should be avoided in order to ensure a fair balancing test is conducted.

Ideally, a data protection subject matter expert should carry out an LIA. However, where this is not possible, an individual with appropriate seniority should be given responsibility to ensure that there is adequate consideration and accountability for the decision-making process.

⁶GDPR Article 6(1)(f)

The 3 key stages of an LIA are:

1. Identify a Legitimate Interest
2. Carry out a Necessity Test
3. Carry out a Balancing Test

The LIA Template ([Appendix B](#)) sets out the key elements of these stages but here are some key considerations at each step:

1. Identify a Legitimate Interest

- The first stage is to identify a Legitimate Interest – what is the purpose for processing the Personal Data and why is it important to you as a Controller? A Legitimate Interest may be elective or business critical; however, even if the Controller’s interest in processing Personal Data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, it must be a 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 is possible that a number of parties may have a Legitimate Interest in processing the Personal Data. While you may only need to identify one Legitimate Interest, all relevant interests should be considered. Your LIA would only cover your relevant processing and the disclosure of the personal data. A Third Party would have to conduct their own LIA for their own processing purposes.

2. Carry out a Necessity Test

Controllers should consider whether the processing of Personal Data is “necessary” for the pursuit of its commercial or business objectives. The adjective “necessary” is not synonymous with “indispensable” but neither is it as wide as “ordinary”, “useful”, “reasonable” or “desirable”. It may be easiest to simply ask, “Is there another way of achieving the identified interest?”

- If there isn’t, then clearly the processing is necessary; or
- If there is another way but it would require disproportionate effort, then you may determine that the processing is still necessary; or
- If there are multiple ways of achieving the objective, then a Data Protection Impact Assessment (DPIA) should be used to identify the 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.

⁶GDPR Article 6(1)(f)

3. Carry out a Balancing Test

A Controller can only rely on a genuine Legitimate Interest where the rights and freedoms of the individual whose Personal Data will be processed have been evaluated, and these interests do not **override** the Controllers’ Legitimate Interest.

- **The balancing test must always be conducted fairly.** The Controller should not attempt to make the assessment unfair or biased, and must always give due regard and weighting to the rights and freedoms of individuals.
- There are several factors to consider when making a decision regarding whether an individual’s rights would override a Controller’s Legitimate Interest. These include:
 - o the **nature** of the interests;
 - o the **impact** of processing;
 - o any **safeguards** which are or could be put in place.

The **nature** of the interests includes:

- **the reasonable expectations of the individual**
 - o would or should they expect the processing to take place? If they would then the impact of the individual is likely to have already considered by them and accepted. If they have no expectation, then the impact is greater and is given more weight in the balancing test
- **the type of data** (i.e. does that data require additional protection under the GDPR, such as data relating to a child or a special category)
 - o Sensitive data is subject to stricter rules on its use. This must be a consideration in a balancing test, and
- **the nature of the interests of the Controller** (e.g. is it a fundamental right, public or other type of interest)
 - o Does it add value or convenience?
 - o Is it also in the interests of the individual?
 - o If there may be harm as a result of the processing, is it unwarranted?

The **Impact** of processing includes:

- 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 Controller needs to carefully consider the likelihood of impact on the individual and the severity of that impact. Is it justified? A much more compelling justification will be required if there is the likelihood of unwarranted harm occurring
- the status of the individual – a customer, a child, an employee, or other
- the status of the Controller – such as, whether a business organisation is in a dominant market position
- the ways in which data are processed, e.g. does the processing involve profiling or data mining? Publication or disclosure to a large number of people? Is the processing on a large scale?

Any **Safeguards** which are or could be put in place include:

- a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing.
- these are likely to have been identified via a Data Protection Impact Assessment conducted in relation to the proposed activity.
- for example:
 - o data minimisation
 - o de-identification
 - o anonymisation
 - o pseudonymisation
 - o privacy by design
 - o adding extra transparency
 - o multi-factor authentication
 - o restricting access rights
 - o data retention limits
 - o opt-out options
 - o encryption, hashing, salting
 - o putting data out of reach
 - o other technical or organisational measures to protect data
- When a Controller is processing Personal Data relating to children, or special categories of Personal Data, special care should be taken with the balancing test, as this may give additional weight to the rights of the individual.

What happens if a balancing test is not in favour of the Controller?

- If the LIA process leads to a negative outcome (i.e. that the Controller cannot rely on Legitimate Interests for the processing operation), the Controller 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 such changes above are not practical, and therefore the outcome of an LIA remains that the Controller cannot rely on Legitimate Interests as a Lawful Basis for the processing, then the Controller must find an alternative legal basis or not proceed with such processing.

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 processing addresses illegal activity it may tip the balance in favour of the Controller, as the Legitimate Interest could be compelling.

What happens if the scope of the processing activity changes?

- An LIA should be revisited if the Controller becomes aware of any of a change in the factors relating to its outcome. The Controller may wish to set review periods for LIAs as a reminder. It will be necessary to conduct a new LIA if the purposes of the processing change.

Please see the LIA Template ([Appendix B](#)) and the Example LIA ([Appendix C](#))



Transparency and the Consumer

Under the GDPR individuals have the right to be informed about how their Personal Data is being processed. The Regulation clearly stipulates that this must be done in a concise, *transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*⁷

Any Controller wishing to rely on Legitimate Interests must inform individuals that it is processing Personal Data on this basis, what the Legitimate Interests are, and also notify individuals of their right to object to processing on these grounds. The information provided to individuals must be explicit, clear and separate from other information.

Informing individuals that you are relying on Legitimate Interests to process their Personal Data, may prove challenging. Controllers may wish to stress that this decision was taken ensuring the privacy rights of individuals were considered and not severely impacted, while emphasising the benefits such processing will provide to customers, supporters, etc.

In order to avoid notices becoming too detailed and difficult for individuals to clearly understand, Controllers may wish to use a layered approach, whereby individuals can click on a link to access more detailed information, should they wish to.

Below are examples of suggested text which could be included in a Privacy Notice which may assist in meeting a Controller's obligation to provide information to individuals. These are provided as examples only – the Controller will need to consider what processing it is doing and whether it is appropriate to rely on Legitimate Interests. Controllers may also wish to refer to the ICO's current guidance on privacy notices - '[Privacy notices, transparency and control](#)'.

Example 1 – Online Privacy Notice

How do we use your personal information? [or similar heading as part of privacy notice]

We may process your personal information for our legitimate business interests.

e.g. fraud prevention/direct marketing/network and information systems security/data analytics/enhancing, modifying or improving our services/identifying usage trends/determining the effectiveness of promotional campaigns and advertising. *[This section should highlight the areas where your business processes data for the purposes of its legitimate interests. Refer to Section [X] for examples of legitimate interests that your organisation may pursue.]*

Click here to learn more about what we mean by legitimate interests, and when we process your data for our legitimate interests.

You have the right to object to this processing if you wish and if you wish to do so please [click here](#)

The first “Click here” takes the visitor to more information (and optional table) where processing activities are set out, along with further details of what legitimate interests means.

“Legitimate Interests” means the interests of our company in conducting and managing our business [to enable us to give you the best service/products and the best and most secure experience].

For example, we have an interest in making sure our marketing is relevant for you, so we may process your information to send you marketing that is tailored to your interests.

It can also apply to processing that is in your interests as well.

For example, we may process your information to protect you against fraud when transacting on our website, and to ensure our websites and systems are secure.

When we process your personal information for our legitimate interests, we make sure to consider and balance any potential impact on you (both positive and negative), and your rights under data protection laws. Our legitimate business interests do not automatically override your interests - we will not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

[Insert optional table, in which organisations may wish to include further detail]

e.g. The table below sets out further detail on the ways we process your data for our legitimate interests. If you have any concerns about the processing below, you have the right to object to processing that is based on our legitimate interests. For more information on your rights, please see “Your Rights” section below.

Example 2 – Online Privacy Notice

We process personal information for certain legitimate business purposes, which include some or all of the following:

- where the processing enables us to enhance, modify, personalise or otherwise improve our services / communications for the benefit of our customers
- to identify and prevent fraud
- to enhance the security of our network and information systems
- to better understand how people interact with our websites
- to provide postal communications which we think will be of interest to you
- to determine the effectiveness of promotional campaigns and advertising.

Whenever we process data for these purposes we will ensure that we always keep your Personal Data rights in high regard and take account of these rights. You have the right to object to this processing if you wish, and if you wish to do so please [click here](#). Please bear in mind that if you object this may affect our ability to carry out tasks above for your benefit.

Example 3 – Data Collection Page

An alternative statement on a data collection page might be:

We may process your personal information for carefully considered and specific purposes which are in our interests and enable us to enhance the services we provide, but which we believe also benefit our customers. [Click here](#) to learn more about these interests and when we may process your information in this way.

Further layers of explanation as outlined above should be available to help inform the consumer fully of the purposes you intend to cover under Legitimate Interests.

Example 4 – Paper Forms

The above examples use a layered approach, which is easily achieved in an online environment. Where the information is being delivered in an offline environment, a “Definitions” section could be included to define Legitimate Interests with an appendix where further details of processing activities could be listed. Controllers may wish to refer to current guidance on drafting privacy notices for more detailed information on this point.

Where Personal Data is being collected offline, it will still be necessary to inform individuals how the Controller may process the information they provide. A balance is required between providing enough information while also ensuring a printed privacy notices do not become too long.

We may process your information for carefully considered and specific purposes to enhance the services we provide. If you would like more information, please visit see our website: [Link to your current Privacy Notice here] or telephone us: [insert relevant name/department and contact number]

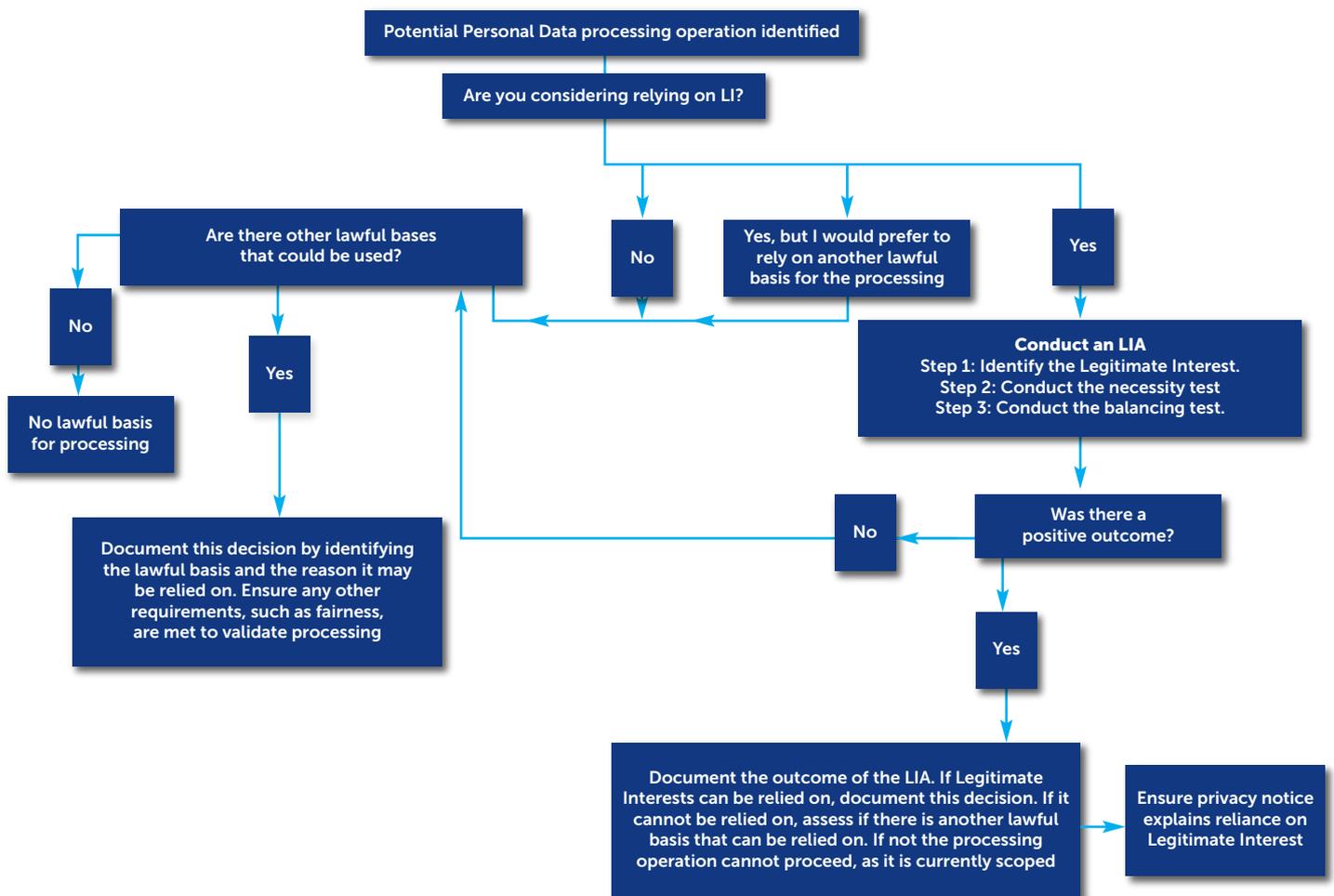
Example 5 – Mobile Format

We may process your data for carefully considered purposes which are in our interests and enable us to enhance the services we provide. [Click here](#) to find out more.



Appendix A

Legitimate Interests (LI) process flow for selecting legal basis for processing





Appendix B

Legitimate Interests Assessment (LIA) Template

Introduction and Instructions

It is worth noting that while this LIA will help you 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.

- The LIA outcome should be documented as evidence and reviewed periodically, particularly where the criteria used in the assessment change materially in any way which could affect the outcome.
- This template should be completed alongside the Data Protection Network's guidance on Legitimate Interests
- This Assessment can be modified to suit your own organisation, for example questions can be added as required from sector to sector.
- The LIA assumes that all other requirements relating to Article 5 of the GDPR (where applicable) have been satisfied. Where possible, evidence should be provided.

A) IDENTIFYING A LEGITIMATE INTEREST			
	Question	Answer	Guidance
1	What is the purpose of the processing operation		The first stage is to identify to a Legitimate Interest – what is the purpose for processing the personal data?
2	Is the processing necessary to meet one or more specific organisational objectives?		If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment. The focus when answering this question should be on your business objectives not the interests of your consumers.
3	Is the processing necessary to meet one or more specific objectives of any Third Party?		For this question, a Third Party is any organisation or individual with whom you may share data with for their own purposes. While you may only need to identify one Legitimate Interest for the purposes of an LIA – the interest that you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party who are likely to have a Legitimate Interest.
4	Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?		For example: Legitimate Interests might be relied on where an individual's (including client or employee) information is processed by a group of companies for the purposes of administration (Recital 48).
5	Why is the processing activity important to the Controller?		A Legitimate Interest may be elective or business critical; however, even if the Controller's interest in processing personal data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, it must be a clearly articulated and communicated to the individual.
6	If applicable, why is the processing activity important to Third Parties the data may be disclosed to?		<p>A Legitimate Interest could be trivial or business critical, however, the organisation needs to be able to clearly explain what it is. Some purposes will be compelling and lend greater weight to the positive side of the balance, while others may be ancillary and may have less weight in a balancing test. Consider whether your interests relate to a fundamental right, a public interest or another type of interest.</p> <p>Just because the processing is central to what the organisation does, does not make it legitimate. It is the reason for the processing balanced against the potential impact on an individual's rights that is key.</p> <p>It is important to consider whose Legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the Personal Data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.</p>
B) THE NECESSITY TEST			
	Question	Answer	Guidance
1	Is there an alternative way to achieve the objective without conducting this processing activity?		<ul style="list-style-type: none"> • If there isn't an alternative, then clearly the processing is necessary; or • If there is an alternative but it would require disproportionate effort, then the processing may still be necessary; or • If there are multiple ways of achieving the objective, then a Data Protection Impact Assessment should have identified the least intrusive means of processing the data which would be necessary

C) THE BALANCING TEST			
	Question	Answer	Guidance
1	Would the individual expect the processing activity to take place?		If the individual would not expect the processing to take place, this could in particular override the Controller's interests. Consider the expectations of the individual, would this processing activity be within their reasonable expectations? Have they been informed? Consider including here any evidence you may have of their expectations that this processing would occur?
2	Does the processing add value to a product or service that the individual uses?		If the processing adds value for the individual this may strengthen the case for Legitimate Interest.
3	Is the processing likely to negatively impact the individual's interests and/or rights?		Consider here whether the processing could lead to discrimination, financial loss, reputational damage, loss of confidentiality or professional secrecy. Or any other economic or social disadvantage. (Please note this is not an exhaustive list). Does the processing prevent data subjects exercising control over their personal data? (See GDPR Recital 75).
4	Would the processing limit or undermine the rights of individuals?		If processing would undermine or frustrate the ability to exercise those rights in future that might well affect the balance.
5	Is the processing likely to result in unwarranted harm or distress to the individual?		
6	Would unwarranted harm or distress to the individual occur if the processing did not take place?		
7	Would there be a prejudice to Data Controller if processing does not happen?		Would there be a negative organisational or commercial impact on the data controller if this processing were not to take place?
8	If applicable, would there be a prejudice to the Third Party if processing does not happen?		Would there be a negative organisational or commercial impact on a Third Party if this processing were not to take place?
9	Is the processing in the interests of the individual whose personal data it relates to?		Focus your response on the customer and any potential benefits of this processing.

C) THE BALANCING TEST			
	Question	Answer	Guidance
10	Are the interests of the individual aligned with the party looking to rely on their legitimate interests for the processing?		<p>What are the benefits to the individual or to society?</p> <p>If the processing is to the benefit of the individual, then it is more likely that Legitimate Interests can be relied on, as the individual's interests will be aligned with those of the Controller. Where the processing is more closely aligned with the interests of the Controller or a Third Party than with those of the individual, it is less likely that the interests will be balanced, and greater emphasis needs to be placed on the context of the processing and relationship with the individual.</p>
11	What is the connection between the individual and the organisation?		<p>Identify the connection:</p> <ul style="list-style-type: none"> • Existing customer • Lapsed/cancelled customer • Employee or contractor • Business client • Prospect (never purchased goods or services) • Supplier • None of above
12	What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?		<p>What types of personal data are being processed e.g. contact data, financial details etc.? Is it data relating to a child? If processing Special Categories of Personal Data, an Article 9 condition must be identified in addition to a lawful basis under Article 6.</p>
13	Is there a two-way relationship in place between the organisation and the individual whose personal information is going to be processed? If so how close is that relationship?		<p>Where there is an ongoing relationship, or indeed a more formal relationship, there may well be a greater expectation on the part of the individual that their information will be processed by the organisation. The opposite is also possible, but it does depend on the purpose of processing.</p> <p>Consider the nature of the relationship, is it:</p> <ul style="list-style-type: none"> • Ongoing • Periodic • One-off • No relationship, or relationship has effectively ceased
14	Has the personal information been obtained directly from the individual, or obtained indirectly?		<p>Consider whether personal information has been collected:</p> <ul style="list-style-type: none"> • Directly • Indirectly • A mix of both <p>If the information was obtained directly from the individual then you should take due consideration of the Fair Processing Notice, the relationship with the individual and their expectations of use. If the data was collected directly and these factors are positive, then it may tip the balance in favour of the processing operation. Where Personal Data is not collected directly, there may need to be a more compelling Legitimate Interest to overcome this. It will also depend on the context of the processing and if the organisation has a two-way relationship with the individual.</p>

C) THE BALANCING TEST			
	Question	Answer	Guidance
15	Is there any imbalance in who holds the power between the organisation and the individual?		If the organisation has a dominant position, this places more responsibility on the Controller to ensure that the interests and rights of the individual are protected. The Controller will need to consider how it addresses any imbalance of power to ensure individuals' rights are not impacted.
16	Is it likely that the individual may expect their information to be used for this purpose?		<ul style="list-style-type: none"> • Yes • No • Not sure <p>Given the relationship between the parties, services/products being provided, including the information notices available, would the individual reasonably expect or anticipate that their information would be used for those or connected purposes? The stronger the expectation, the greater the chances that Legitimate Interests can be relied on.</p>
17	Could the processing be considered intrusive or inappropriate? In particular, could it be perceived as such by the individual or in the context of the relationship?		Processing should not be unduly intrusive - intrusion into the private life of an individual may be justified based on the nature of the relationship or special circumstances. However, the greater the intrusion, perceived or otherwise, the more overwhelming the Legitimate Interest should be and the more the rights of the individual must be considered within the balance. Consider here the way the data is processed (e.g. large scale, data mining, profiling, disclosure to a large number of people or publication).
18	Is a Fair Processing Notice provided to the individual, if so, how? Are they sufficiently clear and up front regarding the purposes of the processing?		Remember that the more unusual, unexpected or intrusive the processing, the greater the importance of making the individual aware of the processing. Particularly where Legitimate Interests are to be relied on.
19	Can the individual, whose data is being processed, control the processing activity or object to it easily?		<ul style="list-style-type: none"> • Yes (cover how you do this in the next section on "Mitigation and Compensating Controls") • No • Partly <p>Giving the individual increased control or elements of control may help a Controller rely on Legitimate Interests where otherwise they could not. If individual control is not possible or not appropriate, explain why.</p>
20	Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?		<p>If yes (cover how you intend to do this in the next section "Mitigation and Compensating Controls")</p> <p>This is a similar concept to a Data Protection Impact Assessment. Where a DPIA might identify potential privacy harms it also allows the organisation to mitigate the risk of non-compliance by adapting or altering the scope of the activity. The same is true for an LIA. If you conclude that the processing presents a privacy risk to the individual, the processing can be limited or adapted to reduce the potential impact.</p>

D) SAFEGUARDS AND COMPENSATING CONTROLS			
	Question	Answer	Guidance
			<p>Safeguards include a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing. These are likely to have been identified via a Privacy Impact Assessment conducted in relation to the proposed activity. For example: data minimisation, de-identification, technical and organisational measures, privacy by design, adding extra transparency, additional layers of encryption, multi-factor authentication, retention, restricted access, opt-out options. , hashing, salting, and other technical security methods used to protect data.</p> <p>Please include a description of any compensating controls that are already in place, or will be put in place, to preserve the rights of the individual.</p>
1	What existing safeguards are in place?		
2	Will any further safeguards be put in place?		
E) REACHING A DECISION AND DOCUMENTING THE OUTCOME			
	Outcome of Assessment:		Guidance
			Using the responses above now document if you believe you are able to rely on Legitimate Interests for the processing operation. Please explain, perhaps using bullet points, why you are, or are not, able to rely on this legal basis. You should draw on the answers you have provided in this questionnaire.
	Signed by:		Role:
	Dated::		
	Review date:		



Appendix C

Legitimate Interests Assessment (LIA) Example to demonstrate how LIA might be used for vehicle telematics

Introduction

The aim of this LIA example is to provide an illustration of how an organisation may approach completing an assessment of their legitimate interests, balancing these carefully with the potential impact on the individuals whose personal data is being processed. This sample is based on one of the case studies provided in [\[insert relevant link\]](#) assessing the use of legitimate interests for vehicle telematics.

The conclusions of any LIA will be subjective and should be based on the experience and judgement of the individual or individuals completing the assessment.

- The LIA outcome should be documented as evidence and reviewed periodically, particularly where the criteria used in the assessment change materially in any way which could affect the outcome.
- An LIA should be completed alongside the Data Protection Network's guidance on Legitimate Interests
- The LIA assumes that all other requirements relating to Article 5 of the GDPR (where applicable) have been satisfied. Where possible, evidence should be provided.

A) IDENTIFYING A LEGITIMATE INTEREST			
	Question	Answer	Guidance
1	What is the purpose of the processing operation	To use telematics to track the location of the controller's vehicle/machine and by association, the driver as a data subject, for the analysis of the performance of the vehicle/machine and of the driver and for the protection of third parties.	The first stage is to identify a Legitimate Interest – what is the purpose for processing the personal data?
2	Is the processing necessary to meet one or more specific organisational objectives?	Yes The processing is necessary for the business to monitor vehicle performance, driver behaviour and ensure road safety	If the processing operation is required to achieve a lawful business objective, then it is likely to be legitimate for the purposes of this assessment. The focus when answering this question should be on your business objectives not the interests of your consumers.
3	Is the processing necessary to meet one or more specific objectives of any Third Party?	Yes, if the Third Party supplies telematics product for the Controller and hosts the information.	For this question, a Third Party is any organisation or individual with whom you may share data with for their own purposes. While you may only need to identify one Legitimate Interest for the purposes of an LIA – the interest that you are seeking to rely on - it may be useful to list all apparent interests in the processing, those of you as the Controller, as well as those of any Third Party who are likely to have a Legitimate Interest.
4	Does the GDPR, ePrivacy Regulation or other national legislation specifically identify the processing activity as being a legitimate activity, subject to the completion of a balancing test and positive outcome?	No	For example: Legitimate Interests might be relied on where an individual's (including client or employee) information is processed by a group of companies for the purposes of administration (Recital 48).
5	Why is the processing activity important to the Controller?	It is important to the Controller for compliance with health and safety legislation, as well as protecting the rights of individuals and for monitoring the performance of employees in accordance with employees' rights. Whilst also ensuring employees comply with the employer's policy in respect of operating vehicles.	A Legitimate Interest may be elective or business critical; however, even if the Controller's interest in processing personal data for a specific purpose is obvious and legitimate, based on the objectives of the Controller, it must be a clearly articulated and communicated to the individual.
6	If applicable, why is the processing activity important to Third Parties the data may be disclosed to?	The machine that is driver operated utilises lithium ion batteries which carries certain risks and tracking the location of the machine is important for responding to machine malfunctions amongst other things	<p>A Legitimate Interest could be trivial or business critical, however, the organisation needs to be able to clearly explain what it is. Some purposes will be compelling and lend greater weight to the positive side of the balance, while others may be ancillary and may have less weight in a balancing test. Consider whether your interests relate to a fundamental right, a public interest or another type of interest.</p> <p>Just because the processing is central to what the organisation does, does not make it legitimate. It is the reason for the processing balanced against the potential impact on an individual's rights that is key.</p> <p>It is important to consider whose Legitimate Interests are being relied on. Understanding this will help inform the context of the processing. In combination with the reason the Personal Data is being processed, this information will determine the weight of the Legitimate Interest that needs to be balanced.</p>

B) THE NECESSITY TEST			
	Question	Answer	Guidance
1	Is there an alternative way to achieve the objective without conducting this processing activity?	We have considered any alternative solutions and can find none that meet our purpose	<ul style="list-style-type: none"> • If there isn't an alternative, then clearly the processing is necessary; or • If there is an alternative but it would require disproportionate effort, then the processing may still be necessary; or • If there are multiple ways of achieving the objective, then a Data Protection Impact Assessment should have identified the least intrusive means of processing the data which would be necessary

C) THE BALANCING TEST			
	Question	Answer	Guidance
1	Would the individual expect the processing activity to take place?	The individual might not expect the use of telematics but we have in place a process to suitably communicate this to driver employees.	If the individual would not expect the processing to take place, this could in particular override the Controller's interests. Consider the expectations of the individual, would this processing activity be within their reasonable expectations? Have they been informed? Consider including here any evidence you may have of their expectations that this processing would occur?
2	Does the processing add value to a product or service that the individual uses?	No	<p>If the individual would not expect the processing to take place, this could in particular override the Controller's interests. Consider the expectations of the individual, would this processing activity be within their reasonable expectations? Have they been informed? Consider including here any evidence you may have of their expectations that this processing would occur?</p> <p>If the processing adds value for the individual this may strengthen the case for Legitimate Interest.</p>
3	Is the processing likely to negatively impact the individual's interests and/or rights?	The risk might be that the location data may identify the driver being somewhere where they are not expected to be, or might infringe their human or data protection rights where they are being monitored using the machine outside of their working hours.	Consider here whether the processing could lead to discrimination, financial loss, reputational damage, loss of confidentiality or professional secrecy. Or any other economic or social disadvantage. (Please note this is not an exhaustive list). Does the processing prevent data subjects exercising control over their personal data? (See GDPR Recital 75).
4	Would the processing limit or undermine the rights of individuals?	No in our assessment.	If processing would undermine or frustrate the ability to exercise those rights in future that might well affect the balance.
5	Is the processing likely to result in unwarranted harm or distress to the individual?	We believe not based on our assessment	
6	Would unwarranted harm or distress to the individual occur if the processing did not take place?	Not in our view.	
7	Would there be a prejudice to Data Controller if processing does not happen?	Yes, the telematics are a risk management tool and also provide protections for citizens who might otherwise not be protected from machine or driver malfunction.	Would there be a negative organisational or commercial impact on the data controller if this processing were not to take place?
8	If applicable, would there be a prejudice to the Third Party if processing does not happen?		Would there be a negative organisational or commercial impact on a Third Party if this processing were not to take place?

C) THE BALANCING TEST			
	Question	Answer	Guidance
9	Is the processing in the interests of the individual whose personal data it relates to?	Yes as it protects them as much as it does the controller	Focus your response on the customer and any potential benefits of this processing.
10	Are the interests of the individual aligned with the party looking to rely on their legitimate interests for the processing	We believe so.	<p>What are the benefits to the individual or to society?</p> <p>If the processing is to the benefit of the individual, then it is more likely that Legitimate Interests can be relied on, as the individual's interests will be aligned with those of the Controller. Where the processing is more closely aligned with the interests of the Controller or a Third Party than with those of the individual, it is less likely that the interests will be balanced, and greater emphasis needs to be placed on the context of the processing and relationship with the individual.</p>
11	What is the connection between the individual and the organisation?	Employee	<p>Identify the connection:</p> <ul style="list-style-type: none"> • Existing customer • Lapsed/cancelled customer • Employee or contractor • Business client • Prospect (never purchased goods or services) • Supplier • None of above
12	What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR?	Employee ID, accompanied by driver statistics. If special categories of data were processed an additional condition for processing would be required separate to legitimate interests.	What types of personal data are being processed e.g. contact data, financial details etc.? Is it data relating to a child? If processing Special Categories of Personal Data, an Article 9 condition must be identified in addition to a lawful basis under Article 6.
13	Is there a two-way relationship in place between the organisation and the individual whose personal information is going to be processed? If so how close is that relationship?	Employer and employee	<p>Where there is an ongoing relationship, or indeed a more formal relationship, there may well be a greater expectation on the part of the individual that their information will be processed by the organisation. The opposite is also possible, but it does depend on the purpose of processing.</p> <p>Consider the nature of the relationship, is it:</p> <ul style="list-style-type: none"> • Ongoing • Periodic • One-off • No relationship, or relationship has effectively ceased
14	Has the personal information been obtained directly from the individual, or obtained indirectly?	Directly, when the individual became a driver employee.	<p>Consider whether personal information has been collected:</p> <ul style="list-style-type: none"> • Directly • Indirectly • A mix of both <p>If the information was obtained directly from the individual then you should take due consideration of the Fair Processing Notice, the relationship with the individual and their expectations of use. If the data was collected directly and these factors are positive, then it may tip the balance in favour of the processing operation. Where Personal Data is not collected directly, there may need to be a more compelling Legitimate Interest to overcome this. It will also depend on the context of the processing and if the organisation has a two-way relationship with the individual.</p>

C) THE BALANCING TEST			
	Question	Answer	Guidance
15	Is there any imbalance in who holds the power between the organisation and the individual?	As an employer we inevitably have the balance of power and as such cannot rely on consent.	If the organisation has a dominant position, this places more responsibility on the Controller to ensure that the interests and rights of the individual are protected. The Controller will need to consider how it addresses any imbalance of power to ensure individuals' rights are not impacted.
16	Is it likely that the individual may expect their information to be used for this purpose?	Yes, as we informed employee drivers.	<ul style="list-style-type: none"> • Yes • No • Not sure <p>Given the relationship between the parties, services/products being provided, including the information notices available, would the individual reasonably expect or anticipate that their information would be used for those or connected purposes? The stronger the expectation, the greater the chances that Legitimate Interests can be relied on.</p>
17	Could the processing be considered intrusive or inappropriate? In particular, could it be perceived as such by the individual or in the context of the relationship?	There is a risk that a driver might be concerned by the concept of monitoring. However, this is balanced by the need to provide an evidential basis that drivers are correctly operating vehicles.	Processing should not be unduly intrusive - intrusion into the private life of an individual may be justified based on the nature of the relationship or special circumstances. However, the greater the intrusion, perceived or otherwise, the more overwhelming the Legitimate Interest should be and the more the rights of the individual must be considered within the balance. Consider here the way the data is processed (e.g. large scale, data mining, profiling, disclosure to a large number of people or publication).
18	Is a Fair Processing Notice provided to the individual, if so, how? Are they sufficiently clear and up front regarding the purposes of the processing?	Individuals will be informed when they undertake a driver induction, as part of this they will receive an employee handbook which gives further information on how their data will be processed.	Remember that the more unusual, unexpected or intrusive the processing, the greater the importance of making the individual aware of the processing. Particularly where Legitimate Interests are to be relied on.
19	Can the individual, whose data is being processed, control the processing activity or object to it easily?	The employees have all the usual rights under applicable law.	<ul style="list-style-type: none"> • Yes (cover how you do this in the next section on "Mitigation and Compensating Controls") • No • Partly <p>Giving the individual increased control or elements of control may help a Controller rely on Legitimate Interests where otherwise they could not. If individual control is not possible or not appropriate, explain why.</p>
20	Can the scope of the processing be modified to reduce/mitigate any underlying privacy risks or harms?	The system has been developed through the concept of privacy by design and as part of this the monitoring facility can be turned off when the vehicle is being operated for personal use.	<p>If yes (cover how you intend to do this in the next section "Mitigation and Compensating Controls")</p> <p>This is a similar concept to a Data Protection Impact Assessment. Where a DPIA might identify potential privacy harms it also allows the organisation to mitigate the risk of non-compliance by adapting or altering the scope of the activity. The same is true for an LIA. If you conclude that the processing presents a privacy risk to the individual, the processing can be limited or adapted to reduce the potential impact.</p>

D) SAFEGUARDS AND COMPENSATING CONTROLS		
Question	Answer	Guidance
		<p>Safeguards include a range of compensating controls or measures which may be put in place to protect the individual, or to reduce any risks or potentially negative impacts of processing. These are likely to have been identified via a Privacy Impact Assessment conducted in relation to the proposed activity. For example: data minimisation, de-identification, technical and organisational measures, privacy by design, adding extra transparency, additional layers of encryption, multi-factor authentication, retention, restricted access, opt-out options. , hashing, salting, and other technical security methods used to protect data.</p> <p>Please include a description of any compensating controls that are already in place, or will be put in place, to preserve the rights of the individual.</p>
1	<p>What existing safeguards are in place?</p> <p>We have policies and procedures to comply with applicable law. We keep personal data no longer than is necessary and store personal data securely.</p> <p>We have in place suitable transparent notices to employees who are drivers of the machines and we limit access to any personal data to a limited number of central employees who manage telematics information.</p>	
2	<p>Will any further safeguards be put in place?</p> <p>We will monitor the telematics and ensure any future versions continue to abide by Privacy by Design. It may be necessary to provide encryption of the telematics information during transition and to provide a mechanism for limiting the collection of personal data and special categories of personal data when the machine is being used outside business hours if appropriate.</p>	
E) REACHING A DECISION AND DOCUMENTING THE OUTCOME		
Outcome of Assessment:		Guidance
<p>Having carried out the above balancing test and LIA we believe that the policies and procedures we have put in place will ensure that our legitimate interests are not overreached by the rights of individuals whose personal data will be processed by the telematics on our machines and vehicles.</p>		<p>Using the responses above now document if you believe you are able to rely on Legitimate Interests for the processing operation. Please explain, perhaps using bullet points, why you are, or are not, able to rely on this legal basis. You should draw on the answers you have provided in this questionnaire.</p>
<p>Signed by:</p>		<p>Role:</p>
<p>Dated::</p>		
<p>Review date:</p>		



Appendix D

The GDPR Articles and Recitals relating to Legitimate Interests

Articles 6(1)(f), 13(1)(d), 14(2)(b), 21(4) 22(2)(b) and 49(1) & Recitals 47, 48, 49, 50 & 68

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"

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;

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(4)

"Right to Object"

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

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

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

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

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

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.

Appendix E

Glossary of Terms

Consent

"Consent" of the data subject means 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 - Article 4(11)

Controller

"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws – Article 4 (7)

Data Portability

The data subject shall have the right to receive the Personal Data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the Personal Data have been provided (see more conditions in Article 20)

Processor

"Processor" means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller – Article 4(8)

Lawful Basis

The term 'Lawful Basis' was used in this Guidance where possible to emphasise that it is part of the 'lawfulness' requirement under the GDPR and to avoid potential confusion with references to a domestic/national legal basis for public task processing.

Legitimate Interests Assessment

A Legitimate Interests Assessment (or LIA) means an assessment carried out by a Controller to decide if a particular processing operation can rely on the Legitimate Interests provision in the GDPR as a lawful basis for processing that Personal Data. This is the same principle found in the ICO and Article 29 Working Party guidance and opinions.

Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person - Article 4(1)

Processing

"Processing" means any operation or set of operations performed upon Personal Data or 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 – Article 4(2)

Special Categories of Personal Data

Article 9 defines special categories of data as "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

Third Party

"Third Party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process Personal Data – Article 4(10)



Copyright of Data Protection Network. All rights reserved. 2018 ©