



**General Data Protection
Regulation (GDPR) Guidance
Note for the Research Sector:
Appropriate use of different
legal bases under the GDPR**

June 2017

Foreword

Jane Frost CBE
CEO, Market Research Society

It's less than a year before the EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018 bringing with it changes in data protection reform across the EU. This will require organisations to become more accountable in protecting the privacy rights of individuals. It is critical that research organisations, of all sizes, continue to take steps to ensure that they are well prepared.

MRS is pleased to be able to share with members this new GDPR Guidance Note tailored for the research sector. Addressing key issues on the appropriate use of legal bases under the GDPR it provides research practitioners with clear guidance on the basic principles of the new GDPR framework focusing on the data processing and collection principles.

The paper is being made available to members of EFAMRO (European Research Federation) and ESOMAR. If you have any specific queries on the document or if you need any additional support please do get in contact with us. Our own Dr Michelle Goddard who is also Director of Policy and Communications with EFAMRO will be happy to assist.



Table of Content

1.	Purpose of Paper	2
2.	Background	3
3.	GDPR at a Glance	5
3.1	Data Protection Principles	5
3.2	Personal Data	6
3.3	Data Controllers and Data Processors	8
3.4	Data Subject Rights	10
3.5	Right to Information and Information Notices	12
4.	Scientific and Statistical Research	16
4.1	EU Research Regime	17
4.2	Member States Research Regimes	18
4.3.	Guidance on Applicability	19
5.	GDPR Processing Grounds for Research	21
5.1	Overview	22
5.2	Consent	24
5.3	Legitimate Interests	29
5.4.	Public Task	34
5.5	Decision Making Tree	35
6.	Tips for GDPR Compliant Scientific and Statistical Research	37
7.	Research Scenarios	39
8.	Appendix	42
	Key GDPR provisions	42

1. Purpose of Paper

The EU General Data Protection Regulation (GDPR) comes into effect in all EU Member States on 25 May 2018.¹

This Paper provides EFAMRO and ESOMAR members with a framework to assist them to:

- ▶ **Understand the basic principles of the new GDPR framework focusing on the data processing and collection principles;**
- ▶ **Determine the appropriate legal grounds to collect, process or further process personal data for all types of research, the conditions that need to be followed and the associated data subject rights; and**
- ▶ **Assess the implications of the different legal grounds for statistical and/or scientific research.**

This data protection guidance is provided as general information for research practitioners. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters.

This is a living document subject to changes based upon data protection guidance and any additional clarifications issued by the Article 29 Working Party (WP29) and/or the European Data Protection Board (EDPB).

Additional joint guidance to be published by EFAMRO and ESOMAR will include a data protection checklist and guidance on conducting data protection impact assessments for research projects.

¹ General Data Protection Regulation 2016/679. Available in all languages in the Official Journal of the European Union L 119 4 May 2016): <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>

2. Background

Collection and processing of personal information is fundamental to the work of researchers. Diverse and evolving techniques, based on qualitative, quantitative or passive methods such as surveys, focus groups, digital measurement, wearable technologies or analytics of large data sets, enable researchers to collect and process personal data to deliver evidence-based insights to clients. All research needs to be based on robust data protection measures to build trust and meet the significant regulatory and legal requirements of the GDPR

Personal data of individual participants (such as contact details) is initially accessed by researchers in several ways:

- ▶ **details on client's customer database;**
- ▶ **panellists provided by a research agency or a client's research panel;**
- ▶ **publicly available data;**
- ▶ **samples provided by a third party; or**
- ▶ **directly from research participants.**

Additional personal data relating to individuals (known as data subjects) such as factual answers, opinions or behaviours and attitudes will then be collected as part of the research process.

Under the GDPR, all researchers, whether employed within an agency, working independently or based within a client's research department, need to ensure that they understand the legal basis being used for collecting, using, storing, sharing or otherwise processing personal data at all stages, as part of their research project.

The paper discusses in detail the following legal grounds:

- ▶ **Consent for general data collection and/or scientific research purposes**

- ▶ **Legitimate interests of the data controller² (which may be a research organisation or a client) and ensuring that in further processing the data is being used for a compatible secondary purpose³**

It also mentions “public task” processing and discusses the special research regime and the specific flexibilities that Member States may add to the GDPR regime for scientific and statistical research.

² Data controller, is the person who alone or jointly with another person, determines the purposes and manner of processing personal data.

³ The other lawful grounds which apply and provide a basis for processing are for performance of a contract, compliance with a legal obligation in EU or Member State (MS) law, to protect the vital interests of the data subject. As these are less likely to be relied on for research purposes these are not addressed in this paper.

3. GDPR at a Glance

In this section we discuss some key data protection concepts focusing on:

- ▶ **the type of data covered by the GDPR;**
- ▶ **who it applies to; and**
- ▶ **the rights given to individuals whose data is covered.**

3.1 Data Protection Principles

The GDPR imposes significant requirements for organisational compliance measures and safeguards such as enshrining privacy by design and default; use of data protection impact assessments (DPIA's); keeping comprehensive data processing records and mandatory reporting of data breaches.

Most importantly the bedrock of the legislation is accountability, requiring that data controllers are responsible for, and are able to demonstrate compliance with, the following six general privacy principles:

- ▶ ***Lawfulness, fairness and transparency*** – Personal data is processed lawfully, fairly and in a transparent manner.
- ▶ ***Purpose limitation*** – Personal data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing is allowed for archiving, scientific, statistical and historical research purposes.
- ▶ ***Data minimisation*** – Personal data processed is adequate, relevant and limited to what is necessary.
- ▶ ***Accuracy*** – Personal data is accurate and, where necessary, kept up to date.
- ▶ ***Storage limitation*** – Personal data is not kept longer than is necessary (but data processed for archiving, scientific, statistical and historical research purposes can be kept longer subject to safeguards).
- ▶ ***Integrity and confidentiality*** – Appropriate technical and organisational measures are put in place to guard against unauthorised or unlawful processing, loss, damage or destruction

3.2 Personal Data

The GDPR covers *personal data* i.e. information relating to an identified or identifiable natural person; who can be identified directly or indirectly by that data on its own or together with other data.⁴

Some personal data is categorised as *special data* and this essentially is sensitive personal data covering religious or philosophical beliefs, health, racial or ethnic origin, trade union membership, political beliefs, sex life or sexual orientation, genetic data and biometric data (including photos when used for the purpose of uniquely identifying a natural person) of individuals. The collection and use of special data is subject to greater restrictions than other types of personal data.⁵

In the research context it is important to recognise that there is a difference between data that identifies a participant in a market, opinion and social research project from data obtained from participants during fieldwork such as responses provided, opinions expressed, etc. The first category of identifiable demographic details (personal data) but the responses of participants will only be considered as personal data when they can be linked to the demographic details (or if the responses themselves have identifiable details within them).

Sound and video recordings and still images should always be considered as personal data in light of the ease of linking these to a person. Ease of technology in doing this means that there is a higher risk of re-identification of this type of materials. Transcripts of recordings should be used in order to properly anonymise them.

Researchers should separate these different categories of information and consider anonymisation of personal data as once you are working with anonymised data (i.e. participant responses which cannot identify an individual), the requirements of the data protection rules are no longer applicable.

Data can also be “pseudonymised”. Pseudonymised data is personal data that has been processed so that it can no longer be attributed to a specific data subject without the use of additional information such as a unique identifier which can make the data identifiable. An original string of data even without the identifier can still be personal data (in the hands of an organisation that holds both the dataset and the identifier) since it can be matched again with the original database to make the data in a string identifiable. In order to become pseudonymised data the additional

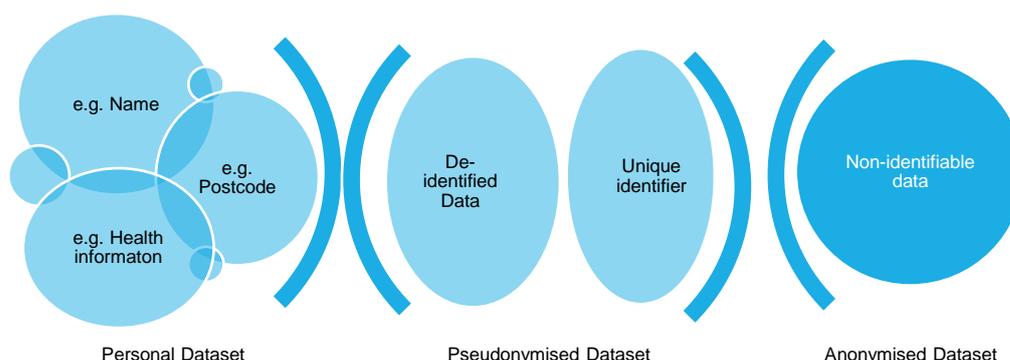
⁴ Article 4 (1) GDPR.

⁵ Information about criminal convictions and offences is treated separately and is subject to tighter controls.

information must be kept separately and held subject to adequate technical and organisational measures. The data can then be considered as pseudonymised data even where the identifier is kept within the same organisation.⁶ Pseudonymised data is still personal data but pseudonymisation of the data is a security technique that provides a mechanism for reducing the level of exposure under the GDPR.

The transition from personal data sets held by researchers through to pseudonymised and anonymised datasets is set out in Figure 1.

Figure 1: From personal to anonymised data



Researchers need to take steps to anonymise data at an early step in the research cycle and follow regulatory guidance to keep up to date with the limits of effective anonymisation in a digital environment.⁷ Regulators do not look to absolute impossibility of identification rather they consider the likelihood of re-identification occurring. In the absence of this pseudonymising or de-identifying data is an important step in the research process. The GDPR sets out a clear preference for processing personal data used in research to the point where data subjects cannot be identified.

Remember also that the GDPR does not apply to data that does not relate to or identify an individual, such as aggregated data sets that show general trends without

⁶ Several techniques available including key-coding, keyed-hashing, introduction of noise etc.

⁷ See ICO Guide to Anonymisation Code of Conduct <https://ico.org.uk/media/1061/anonymisation-code.pdf> and Art. 29 Opinion on Anonymisation Techniques http://www.cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

identifying people or commercial data such as sales or revenue figures which do not contain personally identifiable information.

3.3 Data Controllers and Data Processors

Once you have established that you are processing personal data, you need to establish whether, in carrying out research projects, you are acting as a data controller, a joint data controller or a data processor. More detailed obligations are placed on *data controllers*, who determine the purposes for which the data will be used, than *data processors* but unlike the current Data Protection Directive legal obligations are placed directly on the data processors and all parties involved in the supply chain are potentially liable if the rules are broken. The GDPR applies to processing by businesses operating within the EU and also to businesses that monitor EU residents or offer goods or services to EU residents.

Figure 2: Difference between data controllers and data processors

Data controller	Joint Data Controller	Data Processor
<ul style="list-style-type: none">• If you the researcher determine the purposes and manner in which the data is collected or used	<ul style="list-style-type: none">• If with another data controller such as a client you jointly determine the purposes and manner in which the data is used	<ul style="list-style-type: none">• If you process data on behalf of a controller such as a client or work on research data for a client e.g. transcription, processing, coding, analysing translation, etc

Understanding whether you are acting as a data controller or data processor on the research project will help determine

- ▶ **precisely which accountability obligations under the GDPR are applicable and how this should be reflected in the contract between parties;**
- ▶ **whether and how you can get GDPR consent from the research participants; and**
- ▶ **if GDPR consent is not possible, and you wish to use another legal grounds such as legitimate interests to process data then what needs to be considered before processing the data especially on balancing the interests of the data subject and those of the data controller.**

3.4 Data Subject Rights

Data subjects are living individuals to whom the personal data that is held relates. Under the GDPR these individuals have enhanced rights that allow them to control and protect the use of their data. EU based individuals participating in research will be data subjects with GDPR rights that must be respected.

This is set out in Figure 3 overleaf.

Figure 3: Summary of Individual Rights

Right to Information	<ul style="list-style-type: none">• Extensive information including on all rights, contact details, source, retention period, purposes, categories and recipients etc
Right to withdraw consent	<ul style="list-style-type: none">• Must be as easy to withdraw consent as to give consent
Right to access data	<ul style="list-style-type: none">• Right to access data within 30 days and for free
Right to port data	<ul style="list-style-type: none">• New right to request personal data be provided in usable, transferable format to allow data to move between platforms or suppliers• Applies to data collected by consent or contract
Right to erasure "to be forgotten"	<ul style="list-style-type: none">• New right to erasure of public information held online with absolute right for children• Obligation to inform other controllers to also delete
Right to object to processing	<ul style="list-style-type: none">• Right to object to processing based on legitimate interests or public task• Absolute right to object to processing for marketing and/or profiling• New right to object to processing for research
Right not to be evaluated by automated decision making	<ul style="list-style-type: none">• Right not to be evaluated where decision has legal or significant effects• Not applicable if necessary for contract, authorised by law or based on explicit consent
Right to rectification (of inaccurate data)	<ul style="list-style-type: none">• Right to have records corrected
Right to restrict processing	<ul style="list-style-type: none">• New right to request that processing be restricted where data cannot be deleted as required for legal reasons

3.5 Right to Information and Information Notices

The strengthened right to information sets out extensive information requirements where data is obtained directly or indirectly from a data subject.

This is set out in Table 1 overleaf which has been reproduced from the UK's data protection regulator's guidance, ICO Overview Guide on Individuals Rights⁸

⁸ See further <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/>

Table 1: Extract from the UK ICO Overview Guide on Individual Rights

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
--------------------------------------	------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Provision of the information required in notices will require tailoring and a creative approach to ensure that the transparency purpose is adequately fulfilled. Information notices will take various formats and depending on the type of research may be published by research clients and/or published and circulated by researchers directly to research participants. In some projects they will be provided as part of the process of gaining informed consent and in other cases will be provided to let individuals know how their personal data will be used.

Researchers must ensure information notices are:

- ▶ **written clearly in an accessible manner that takes into account the audience likely to be reading the notice.**
- ▶ **appropriately tailored to the platform that the information is being conveyed on. In digital environments this can be achieved by using layered notices that provide a short condensed overview of the notice with innovative techniques used to direct readers to the full notice. Use of explanatory videos should be considered. In telephone research opportunity can be taken to direct participant to further information on a website; to a nominated individual for queries or to reduce the upfront information burden by providing some information at the start of a phone call and conveying the rest at the end of a call.**

4. Scientific and Statistical Research

The GDPR has specific provisions for scientific and statistical research that researchers must comply with in processing personal data. The meaning of these research purposes is set out in the introductory text of the GDPR:

- ▶ **Scientific research purposes – this is to be interpreted in a broad manner to “include” privately funded research.⁹ The GDPR definition is not exhaustive but indicative of types of research using terms “such as” and “in particular” which do not preclude the inclusion of commercial research. Some commercial research is expected to fall within scope.**
- ▶ **Statistical research purposes – this means “any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results.” This will cover research that results in aggregate data that is not used to support measures or decisions regarding an individual. The outputs of statistical research can also be further used for other purposes including scientific research.¹⁰**

⁹ Recital 159

¹⁰ Recital 162

4.1 EU Research Regime

The research regime set out in Article 89 expressly allows across the EU:

- ▶ **broad consents for scientific research where consent cannot be secured for all specific purposes at the outset of data collection;**¹¹
- ▶ **further use of personal data for scientific or statistical research as a secondary compatible purpose**¹²;
- ▶ **the right of the data subject to object to processing of personal data (unless necessary in public interest)**¹³;
- ▶ **restriction of the right of a data subject to exercise their “right to erasure” if it is likely to significantly impair processing for scientific research purposes;**
- ▶ **relaxation of the storage limitation principle granting the ability to store personal data for longer periods;**and¹⁴
- ▶ **isolated transfers of personal data to third countries taking into account legitimate expectations of society for an increase in knowledge.**¹⁵

Additionally information obligations in scientific research do not apply if they would involve a disproportionate effort. Consideration of this takes into account the number of data subjects and the age of the data and appropriate safeguards must be adopted.¹⁶ Furthermore there is “no right to be forgotten” if it is likely to significant impair processing for scientific research purposes.¹⁷

Use of the Article 89 research regime is subject to certain conditions:

- ▶ **Appropriate safeguards to protect the right and freedoms of the data subject.**
- ▶ **Adequate technical and security measures entrenching the principle of data minimisation and using pseudonymised data as default.**
- ▶ **Compliance with recognised ethical safeguards.**

¹¹ Recital 33

¹² Article 5(91)(b); Recital 50 sets out the compatibility test. It is likely that market, opinion and social research will still be considered a compatible purpose under the test set out in the Regulation regardless as to whether it is specifically included within the definition of scientific research. However if it is not considered to be statistical research or scientific then researchers need to adopt the balancing test and criteria set out in Article 6(4).

¹³ Article 21(6)

¹⁴ Article 5(1) (e)

¹⁵ Recital 113

¹⁶ Article 14(5); Recital 62

¹⁷ Article 17(30); Recital 65

4.2 Member States Research Regimes

The research regime also allows Member States (MS) to make specific provisions on:

- ▶ ***ability to process sensitive categories of data*** - National legislation can provide that sensitive data may not be processed or impose additional conditions for processing biometric, genetic or health data. It can also confirm that scientific research is a legal processing grounds for use of this type of personal data.
- ▶ ***Restrictions of five individual rights*** – Rights to access data; to rectify inaccurate data; to restrict processing; to object to processing; and the right of a child to be forgotten (if necessary for the processing) can be restricted for research purposes. Each Member State can choose which individual rights will be limited in their national law. States can independently decide to limit all, none or some of these rights.

Member States are allowed to provide for additional safeguards and to set out conditions and safeguards for any national derogations/exemptions granted.¹⁸

Additionally, where personal data is processed for statistical purposes, Member States and/or union law will determine statistical content, control of access, specifications for processing and measures to safeguard individual rights and freedoms and to ensure statistical confidentiality.¹⁹

The national research regime allows significant relaxation of several individual rights (but consideration should always be given by the researcher at each point as to whether the restriction of the data subject right is necessary).

¹⁸ Recital 156

¹⁹ Recital 162

4.3. Guidance on Applicability

In order to secure a harmonised and consistent framework it would be useful for the special research regime under Article 89 to be applied consistently across the EU especially with regards to the general conditions and safeguards for processing. This position is currently being sought via representations being made within Europe by EFAMRO and ESOMAR.

The status of the research regime is currently an open question. Some experts consider that the research regime can serve as a legal gateway for processing personal data. This would mean that if conducting scientific research the approach under Article 89 would be the default position. Other interpretations of the research regime are that it provides a back-up position when personal data cannot be processed for research purposes on one of the other legal bases.

Clear requirements for Article 89 safeguards should be established and applied. In the current absence of regulatory guidance on this point this paper sets out proposed best practice for researchers in line with the GDPR provisions. These will be revised, as necessary, in line with ongoing discussions with the national regulatory authorities and guidance issued by the WP29 group of European data protection regulators.

- ▶ ***Is commercial research within the research regime?*** The recitals provide guidance and indicate a broad interpretation that should bring commercial research within the regime. The GDPR definition is not exhaustive but indicative of types of research using terms “such as” and “in particular” which does not preclude inclusion of market, opinion and social research.
- ▶ ***What ethical safeguards are required?*** Researchers currently abide by national and/or international research codes such as the ICC/ESOMAR International Code on Market and Social Research or the MRS Code of Conduct in the UK. Ethical safeguards under the GDPR are likely to extend to established self-regulatory codes of conduct as well as academic ethics reviews.
- ▶ ***Is intended publication of the research necessary?*** The recitals note that scientific research should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area which may suggest that research should be made publically available. As a significant amount of the commercial research conducted by EFAMRO and ESOMAR members is intended for internal use of clients an interpretation on this basis would limit the utility of the research regime. It would however apply to significant amounts of public sector research where publication of research results is more usual.

Full adherence to the spirit and letter of the data protection principles is critical in creating a compliant research environment. Key aspects of these areas will be addressed in future guidance by EFAMRO and ESOMAR.

Active consideration is also being given to the development of a GDPR Code for market, opinion and social research, to be submitted to the European regulators for approval as part of their Code approval process and will provide regulator approved detailed guidance for the research sector. Such an approach would significantly strengthen the research sector's current self-regulatory compliance framework.

5. GDPR Processing Grounds for Research

In order to process personal data at least one legal processing ground must be satisfied. Data controllers must choose the most appropriate ground for the data processing. It is important to stress that under the GDPR there is no hierarchy of processing grounds. The key point is to ensure that the right ground is chosen for the data processing activity and that this is detailed in internal data processing records.

5.1 Overview

The grounds that researchers can use to process personal data are:

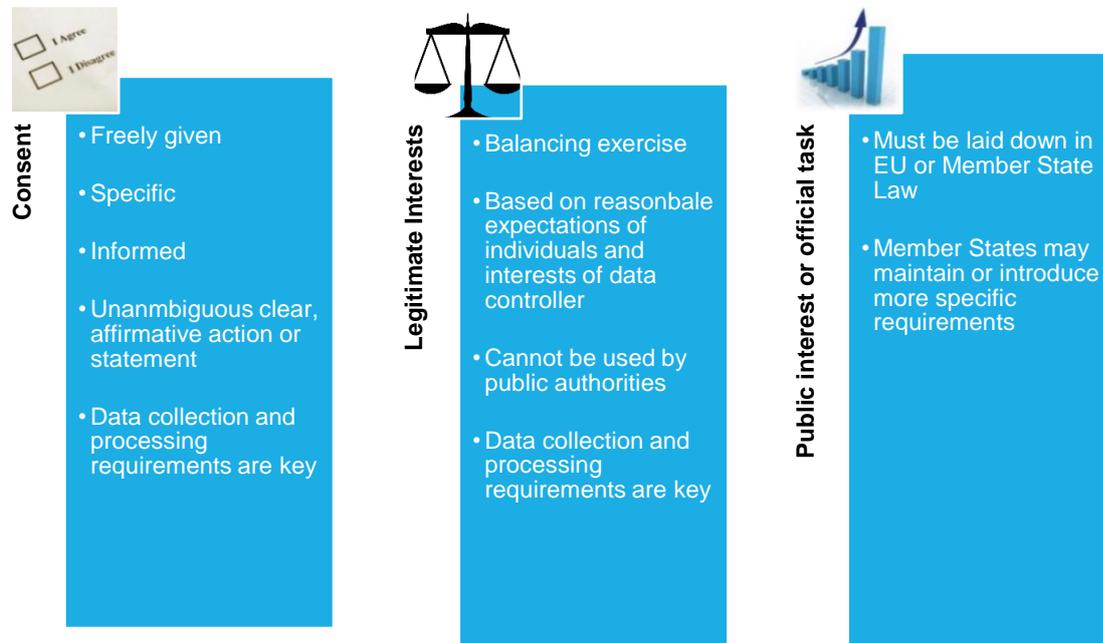
- ▶ **consent of the data subject/ research participant for the research purpose(s);**
- ▶ **legitimate interests of the data controller (or a third party). In determining what these legitimate interests are you need to ensure that you balance the interests of the controller with any prejudice to the rights and freedoms or the interests of the data subject. In assessing whether the data controller has a legitimate interest you need to take into account the reasonable expectations of the data subject. Public authorities cannot base processing on this ground; and**
- ▶ **performance of a public interest task or exercise of official authority.**

In line with the ethical standards set out in national and international research codes of conduct, consent of research participants will be critical for a significant amount of market, opinion and social research in many EU Member States. However the approach taken varies by Member States as domestic markets for research have different characteristics. Researchers need to assess what grounds are most used and useful within their individual jurisdiction and comply with any national research code of conduct in addition to the requirements of the GDPR. For example in the Netherlands grounds such as legitimate interest or consent are used less frequently, whereas in Germany consent is the primary legal basis under which market, opinion and social research is undertaken.

The bar chart in Figure 4 overleaf illustrates the grounds likely to be used to process personal data for research purposes across the EU.²⁰

²⁰ Special research regime is not a separate legal ground but provides researchers with the ability to process personal data that has been otherwise lawfully obtained.

Figure 4: Illustrative Research Processing Grounds



5.2 Consent

Obtaining consent under the GDPR is more difficult as the test is higher than the requirements of the Data Protection Directive. Consent is about choice and control, and although it will often be the right lawful basis for carrying out research, researchers must be certain that consent is the most appropriate ground for the research project. In particular you must ensure that consent is:

- ▶ **given by clear affirmative statement or action and clearly distinguished from other terms and conditions. Silence, pre-ticked boxes or inactivity cannot be used to give consent; and**
- ▶ **specific to the purpose which must be highlighted to individuals.**

Consent can be used for all types of data collection and researchers can also use the slightly less restrictive consent regime set out in Table 3 where undertaking scientific research.

Table 2: Using consent for general data collection

Suitable for research approaches such as:

- ▶ Panel research
- ▶ Qualitative and quantitative research based on free-found recruitment; random dialled telephone interviews
- ▶ Customer satisfaction research (not from client databases)
- ▶ Online surveys e.g. web based; audience measurement surveys
- ▶ Demographic segmentation based on research surveys
- ▶ Tracking based digital market research²¹

Conditions

If as a researcher you use consent for data collection you need to be aware of the following:

Consent must be:

- ▶ freely given
- ▶ specific - can cover multiple processing purposes including the research purpose – but must be highlighted from any other terms
- ▶ informed
- ▶ unambiguous indication with clear affirmative action or statement

Data controller needs to be able to demonstrate that consent was obtained.

Data Subject Rights

If you use consent for data collection need to ensure that data subjects have the right to the following information:

- ▶ **identity of data controller**
- ▶ **contact details of data protection officer**
- ▶ **legal basis for processing;**
- ▶ **purposes of processing;**
- ▶ **details of any international data transfer;**
- ▶ **retention period for data or criteria for retention;**
- ▶ **existence of any automated decision making and logic, significance and consequences**
- ▶ **details of all other rights including right to object, right to data portability, right to withdraw**

²¹ The EU Commission has published a proposal to reform the e-Privacy Directive. The proposed ePrivacy regulation will have a significant impact on online research..

Forms of consent

Consent may be given:

- ▶ in writing
- ▶ electronically; or
- ▶ orally

Children

Age verification is required for parental consent for children either as set out:

- ▶ in contractual law of (MS) or
- ▶ for online “information society services” those under 16 (or under 13 depending on national law).

Explicit for sensitive data

If processing special category/sensitive data then consent must

- ▶ be explicit
- ▶ follow any additional provision in MS law for sensitive personal data

Profiling

If conducting research using *profiling or segmenting* and making decisions based on this then additional restrictions will apply.

consent; right to lodge complaints with supervisory authorities

This information must be set out in clear and plain language. Take note of regulatory guidance on privacy notices in conveying the information.

Data subjects also have other rights:

- ▶ **to withdraw consent at any time (must be as easy to take away as to give)**
- ▶ **to port data (if automated information collection) but unclear whether this will apply in a research context**
- ▶ **to erasure of data made public (and data controller will need to inform other controllers who may be processing)**
- ▶ **to restrict processing**
- ▶ **to access data**
- ▶ **to rectify data held**
- ▶ **to object to the processing**
- ▶ **to not be subject to decision based on automated processing (including profiling) which produces legal effects or significantly affects them.**

All of the rights must be promoted at each contact point.

Researchers using consent for research purposes can seek broad consent from data subjects for research activities. This means that you can store data for longer, restrict the right of the individual to have their data erased and also restrict the right of the research participant to object (once the research is in the public interest). For archival research projects you can also restrict the right to data portability.

Table 3: Using consent for scientific and statistical research purposes

Suitable for research approaches such as:

- ▶ Published social research projects
- ▶ Public health research
- ▶ Longitudinal studies

Conditions

If as a researcher you use broad consent for scientific and statistical research purposes you need to be aware of the following:

Broad consent can be obtained from participants where:

- ▶ It is not possible to identify all purposes of personal data processing for scientific research purposes at time of data collection²²

Researchers must :

- ▶ follow ethical standards for scientific research and implement technical and organisational safeguards

Researchers may, if appropriate,

- ▶ store personal data for longer periods

Data Subject Rights

If you use consent for scientific or statistical research purposes data subjects have general individual rights but researchers, across the EU can restrict the following rights :

- ▶ **data subjects right to have their data erased (where it may impact on the integrity of the research)**
- ▶ **data subjects right to object to processing for research purposes (if necessary for public interest reasons).²³ Decision taken on this is subject to a balancing test and the burden is on the researcher to demonstrate compelling grounds for continuing with the research**
- ▶ **additional rights may also be restricted under national research regimes.**

²² Recital 33

²³ Article 21

5.3 Legitimate Interests

Under the GDPR researchers can conduct research based on the legitimate interests of the data controller (or third parties) except where such interests are overridden by the fundamental rights and freedoms of the data subject. Particular care should be taken in considering the rights of children.

Researchers using this ground need to be clear as to who is the data controller and understand exactly what the data controller's legitimate interests are so that they can undertake a balancing test. Adopt a logical approach to using this ground as follows:

- ▶ ***Determine whose legitimate interests*** - The legitimate interests may be those of the researcher acting as a data controller such as where a research agency recalls participants for quality control purposes, (even where they have not consented to a recall for research). It may also be the legitimate interests of the client such as when a researcher is contacting client's customers on a database. It may also be a researcher's interest as a third party to access a database.
- ▶ ***Determine if the processing is necessary to pursue the interest*** – Consideration of the proportionality of the processing is important. Can the objectives be achieved with the collection of less data? Are there more privacy enhancing means of processing the data for this purpose?
- ▶ ***Balance the interests of data controller with interests of data subject*** – Assess whether the data controller's interest is overridden by fundamental rights and interests of the data subject. It is important to look at the impact on data subjects, the way the data is being processed and the reasonable expectations of data subjects. Balancing the data controller's rights against the rights of the individual in a research context means that you should attempt to structure and carry out the research in the least intrusive and most privacy-enhancing way. Remember also that the rights of the individual are paramount to that of the research organisation.
- ▶ ***Document the balancing process*** – Keep a written record of reasons why you feel the balancing test was met. This important in order to meet the GDPR accountability principle.

In line with previous opinions of WP29 (under the current Data Protection Directive) market, opinion and social research on client's customers is) within the reasonable expectations of customers. So although research is not specifically mentioned in the GDPR as a legitimate interest (although direct marketing is) it is expected that market, opinion and social research activities will fall within this ground.²⁴

Additionally WP29 has previously noted that under the Directive processing for historical, scientific or statistical purposes and for research purposes (including marketing research) are contexts where legitimate interests can arise.²⁵

This ground however cannot be used for research by public authorities or for decisions based on profiling activities.

²⁴ See also Art. 29 Working Party on legitimate interests and Directive which specifically mentioned market research http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf

²⁵ See Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

Table 4: Using Legitimate Interests for Data Collection

Suitable for research approaches such as:

- ▶ **Customer satisfaction research (on existing customer databases)**
- ▶ **Quantitative or qualitative research using customer databases**
- ▶ **Research using existing data sets or third party data (i.e. data not directly provided by individual or where no contractual relationship) such as social media analytics**
- ▶ **Data analytics on loyalty card data**
- ▶ **Possible feasibility of use for Big Data projects i.e. data analytics of mixed brand datasets customer behaviours, preferences and movements. If unable to contact all participants then need to use the flexibility in the information obligations where contacting all participants for scientific research would involve a disproportionate effort.**

Conditions

If as a researcher you use legitimate interests for data collection you need to:

- ▶ Consider either yourself (if you are data controller) or with client (if they are the data controller) what the reasonable expectations of the data subject are at the time of data collection and balance interests
- ▶ Ensure that the Privacy/Fair Processing Notice detail the legitimate interests pursued by the controller. This is different from a consent notice which requires affirmative agreement.
- ▶ Consider whether you or the client need to provide an updated Notice. This may be the case if the data is to be used for new purposes e.g. where research was not initially mentioned.

Data Subject Rights

General individual rights apply as with consent but data subjects have:

- ▶ right to object to processing on this ground can be exercised without providing specific reasons
- ▶ right to be notified about right to object at time researcher communicates with participant

Also individuals do not have a right to port or move their data (as this only applies where data gathered on the basis of consent or contract)

Updated notices must include original notice requirements.

- ▶ Document your analysis and maintain a written record of your analysis that details the reasons why you reached the conclusion that the balancing test was met. This must be done in order to meet accountability principle.
 - ▶ Legitimate interests cannot be used as ground for collecting special category of personal data.
-

Secondary use of personal data for research purposes

Legitimate interests can also be used to process data further within the reasonable expectations of data subjects. If personal data being processed, has not been collected by consent, then the processing can only be for a compatible purpose.

Key points in determining compatibility are (this is not a limited list):

- ▶ **Link between purposes**
- ▶ **Context and relationship between data subject and data controller**
- ▶ **Nature of personal data**
- ▶ **Possible consequences of processing**
- ▶ **Safeguards used such as encryption/pseudonymisation**

Therefore researchers can use personal data for secondary research purposes based on the legitimate interests of clients as research purpose is likely to be compatible with original data collection and processing purpose; or if it is scientific/statistical research it is deemed compatible.

5.4. Public Task

Researchers conducting research for public authorities will not be able to rely on legitimate interests and may need to base processing on “performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

Article 6(3) and Recital 45 make clear this ground will apply only where the task carried out, or the authority of the controller, is laid down in Union law or Member State law to which the controller is subject.

As such this may be a restrictive ground for processing. More detailed guidance will be provided on this after consultation with regulatory authorities and national research institutions producing official government statistics.

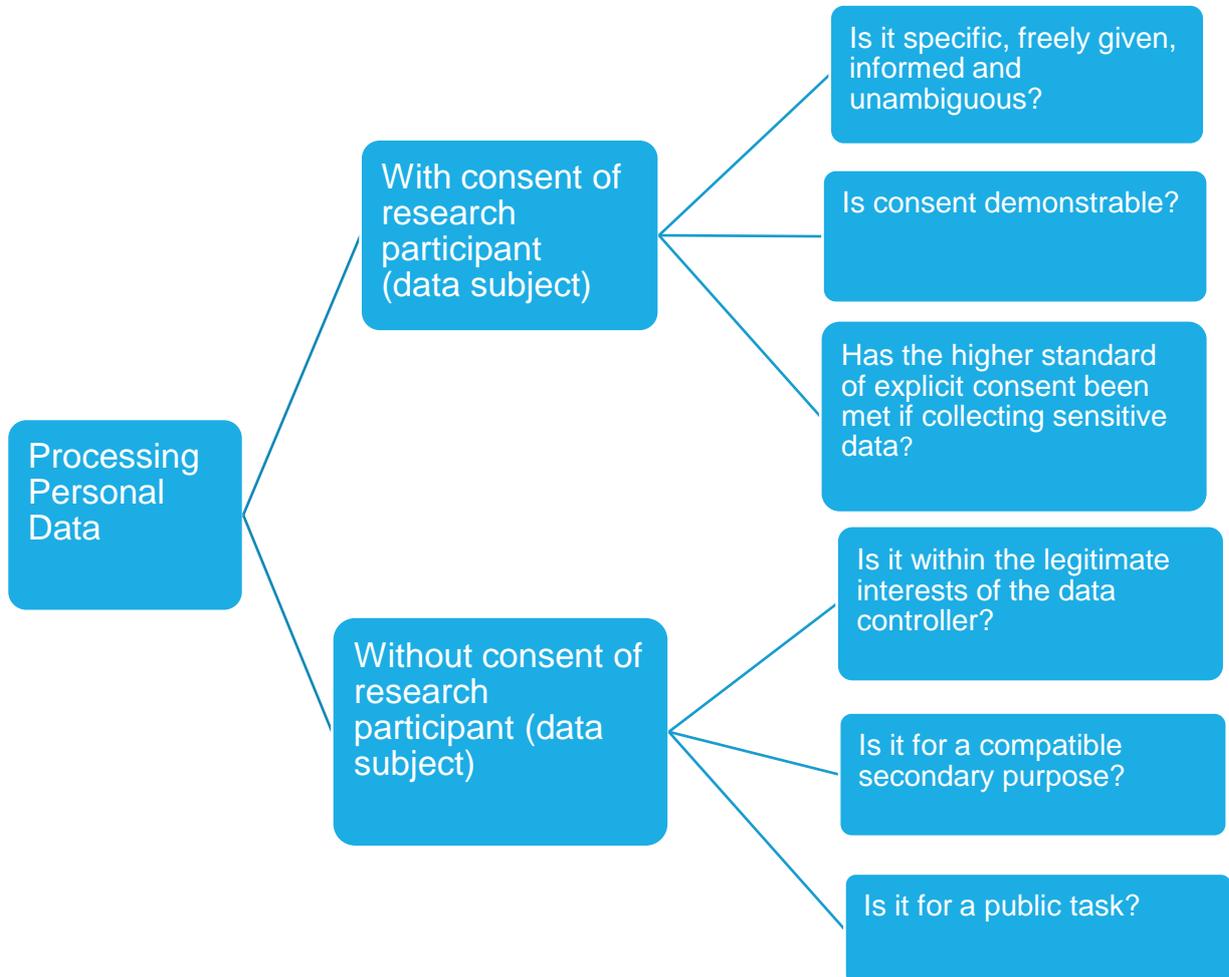
5.5 Decision Making Tree

If collecting or using participant's personal data, researchers need to ask a series of questions to assess the appropriate legal ground:

- 1. *Are you a data controller or a data processor?*** If the client is the data controller, responsible for determining the purposes of the research exercise, or joint data-controller with you then this may impact on your choice of processing ground for the research.
- 2. *Can you obtain consent from research participants?*** Can you get freely given, specific, informed and demonstrable consent for the research? Or can you get broad consent for a scientific research purpose? Research will be allowed.
- 3. *If you can't get consent can you rely on other grounds?*** Can you use the legitimate interests of the data controller or the public interest of a public authority?
- 4. *Are you sure that the research falls within the legitimate interests of the data controller?*** Secondary processing can be based on the compatibility of the market /social research project with the data controller's interests (after checking to see what the participant has been told the data will be used for). This is not available to public sector bodies.
- 5. *Is this research a new secondary use of the personal data?*** In order to further process the personal data you need to ascertain whether the new purpose is compatible with the original purpose. If it is for scientific research purpose the research will be compatible and allowed. If it is for general data collection you will need to consider compatibility of the new use and consider where it falls within the reasonable expectations of the data subjects.
- 6. *Is the research necessary for performance of a task carried out in the public interest or under official authority?*** Public interest grounds will need to be relied on by public authorities if they cannot use consent.

Once you have identified a lawful ground to process the data the next step is put in place technical and organisational measures and follow ethical safeguards whilst conducting the research.

Figure 6 Decision Making Tree



6. Tips for GDPR Compliant Scientific and Statistical Research

In a research context some of the specific issues that should be considered in complying with general data protection principles are:

- ▶ **Lawfulness, fairness, and transparency** – Information notices such as informed consent forms need to be clearly written and presented. Ensure that clients have explained in their privacy policies and notices what they consider their legitimate interests to be and included research activities in these.
- ▶ **Data minimisation** - Researchers should strive to minimise the amount of personal data held. De-identify or pseudonymise data by removing identifying details as early in the process as is feasible. Personal data for research purposes is often only required at the outset of the project. Apart from panel providers and social media research, market, opinion and social research activity rarely needs to retain the personal data once fieldwork, quality control checks and payments for incentive have finished. If a participant communicates his/her opposition to the processing of his/her data, the researcher will need to facilitate this by not further processing identification data. However if the responses have already been incorporated and anonymised or aggregated in a market, opinion or social research project, then that data does not have to be deleted as it not personal data.
- ▶ **Storage limitation** – GDPR allows data for scientific research purposes to be held for longer periods. However as data subject rights apply where personal data is held steps should be taken to minimise the level of personal data held for research purposes. It is only applicable to personal identifiable data and not to responses that cannot be linked. Retention periods should be established for personal data, and data subjects informed of the period or the criteria used in deciding how long the data will be kept for. In the absence of an agreement with a client ISO 20252 provides that primary records (which typically contain personal data) should be held for a year. Researchers can agree longer or shorter periods where necessary. Retention periods should only be for as long as the personal data is required.
- ▶ **Accountability** - Records of decision made on legitimate interests, data protection impact assessments and the appointment or non-appointment of a Data Protection Officer are all important in demonstrating accountability. IT systems need to be able to record and demonstrate consents and facilitate the exercise of all individual rights including rights to access data and withdraw from the research at any time.

7. Research Scenarios

The scenarios in this section illustrate some of the points to think about in reviewing the legal ground for collecting personal data for research purposes.

Scenario 1 - Consent

Digital Brand DEF has commissioned a Research Agency to provide insights on its digital service working with a new brand-specific online community established for this purpose. The Agency has been given freedom to determine what issues to raise with members of the community. It is considering sub-contracting with a US-based agency to host the online community.

Key points to consider:

▶ **Who is the data controller?**

Research agency will be the data controller or joint data controller with the client as has freedom in determining how and when to collect personal data.

▶ **What is the legal basis for the research?**

Participation will be based on the tighter consent rules under the GDPR.

Clear and comprehensive information notices must be provided to participants before research project begins to get consent.

Consent form must include full list of information including retention period, identity of controller and the jurisdiction in which the data will be processed or stored etc.

Care must be taken in presenting the key information e.g. highlighted links with links to other relevant information, innovative techniques such as just in time notices.

Consents must be recorded and need to ensure can provide audit trail of consent and that IT system allows participants to exercise all rights including access to data and withdrawal from research.

▶ **Is the data transfer adequate?**

If a US-based processor is used and personal data is being stored/processed in the US then you need to consider whether the data transfer is adequate. Is the processor Privacy Shield certified? The position with data transfers especially to the US is fluid and sufficiency of this should be under regular review. Contracts with data processors must be in writing and include mandatory GDPR clauses.

Scenario 2 - Legitimate Interests

Research Agency has been commissioned by Brand ABC to carry out a confidential online customer satisfaction survey on its behalf. The survey has been written by the client and loaded on to the Research Agency's data collection system with a hyperlink sent for survey collection. The research agency will analyse responses and report back aggregated responses to the client.

Key points to consider:

▶ Who is the data controller?

Research agency is a data processor as it does not determine the purposes for which the data will be used or the manner in which it will be used. The client will be the data controller.

▶ Which legal basis can be used for the research?

Legitimate interests can be used as a legal ground and will be based on the legitimate interests of the client. Contacting customers on a brand database for research purposes will normally be able to rely on this ground.

Researcher must:

- make sure that the brand's external privacy notice specifically sets out that personal data collected will be used for research purposes and setting out reasons why the Brand considers it as a legitimate use of personal data.
- treat cookies, device ID's etc collected as personal data.
- respect all the participants right including the right to object to processing (without any specific reasons).

Researcher should consider whether need to get informed consent for the research at the point of data collection for the research exercise in line with any relevant research Code requirements.

Alternatively, the statistical research regime can also be used as a legal ground once there will be aggregated reporting of the data. Data must be pseudonymised and kept secure.

Scenario 3 - Big Data and Legitimate Interests

A large Supermarket chain has commissioned a research agency to carry out research and link to existing datasets. The agency will link datasets including new research data, demographic, transactional and usage data of customers and report back to client.

What is required for this to be done in line with GDPR requirements?

Key points to consider:

▶ Who is the data controller?

Research agency will be joint data controller with the client as has freedom in determining how and when to collect the personal data for research project.

▶ Which legal basis can be used for the research?

Processing data in this way can be based on legitimate interests of the supermarket. Repurposing personal data collected for other purposes such as the transactional and usage data is possible once the processing is considered compatible. It is expected that market research will be considered compatible but it cannot be an onerous intrusion into an individual's privacy.

Researcher will need to balance the interests of business with those of the data subjects giving primacy to fundamental individual rights.

Researcher needs to:

- make sure that the brand's privacy notice specifically set out that research is considered as a legitimate use of each dataset.
- ensure that the research design is privacy enhancing
- preferably report aggregated data
- implement appropriate technical safeguards such as hashing of personal data or key coding of data sets
- Undertake a Data Protection Impact Assessment to assess and mitigate any high privacy risks e.g. if undertaking non-market research such as creating identifiable customer segments to target individual consumers additional rules will have to be followed.

8. Appendix

Key GDPR provisions

Recitals

Recital 26

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Recital 33

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

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.

Recital 52

Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

Recital 53

Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the

general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

Recital 62

However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

Recital 65

A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise

that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

Recital 113

Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

Recital 156

The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to

appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

Recital 159

Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, **the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.** In addition, it should take into account the Union's objective under Article 179(1) TFEU²⁶ of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.²⁷

Recital 162

Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes,

²⁶ Article 179 (1) of the TFEU promotes “the objective of strengthening its scientific and technological basis by achieving a European research area in which researchers, scientific knowledge and technology circulate freely” which suggests that the research should be published or made otherwise available [but this is open to interpretation](#).

²⁷ Healthcare research is included in scientific research but there are additional provisions applicable only to public health research.

including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

Article 5 Principles relating to processing of personal data

Personal data shall be:

- a. **processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**
- b. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');**
- c. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');**
- d. **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');**
- e. **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');**
- f. **processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using *appropriate technical or organisational measures ('integrity and confidentiality')*.**

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Articles

Article 4 Definitions

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 6 Lawfulness of processing

1. 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. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
 - (a) Union law; or
 - (b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
 - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
 - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
 - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
 - (d) the possible consequences of the intended further processing for data subjects;
 - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 9 Processing of special categories of personal data

1. Processing of personal data revealing 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 shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued,

respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 14 Information to be provided where personal data have not been obtained from the data subject

5. Paragraphs 1 to 4 shall not apply where and insofar as: (a) the data subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 17 Right to erasure ('right to be forgotten')

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.

Article 21 Right to object

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 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.



Founded in 1992, EFAMRO represents the interests of market, social and opinion research in Europe. Its members are national trade associations for research businesses. For further information on EFAMRO and its activities, contact Dr Michelle Goddard, Director of Policy and Communication.

EFAMRO
Bastion Tower, level 20 Place du
Champ de Mars 5, B-1050 Brussels

T : +32 (0)2 550 3548

www.efamro.eu

F : +32 (0)2 550 3584

E : michelle.goddard@efamro.eu



Founded in 1948, ESOMAR gathers nearly 5000 professionals and over 300 companies worldwide providing or commissioning research, including public and academic bodies. For further information on ESOMAR and its activities, contact Kim Smouter-Umans, Head of Public Affairs and Professional Standards.

ESOMAR
Atlas Arena, Hoogoordreef 5, 1108 BA
Amsterdam, The Netherlands

T: +31 20 664 2141

F: +31 20 664 2922

E : public.affairs@esomar.org

W : www.esomar.org