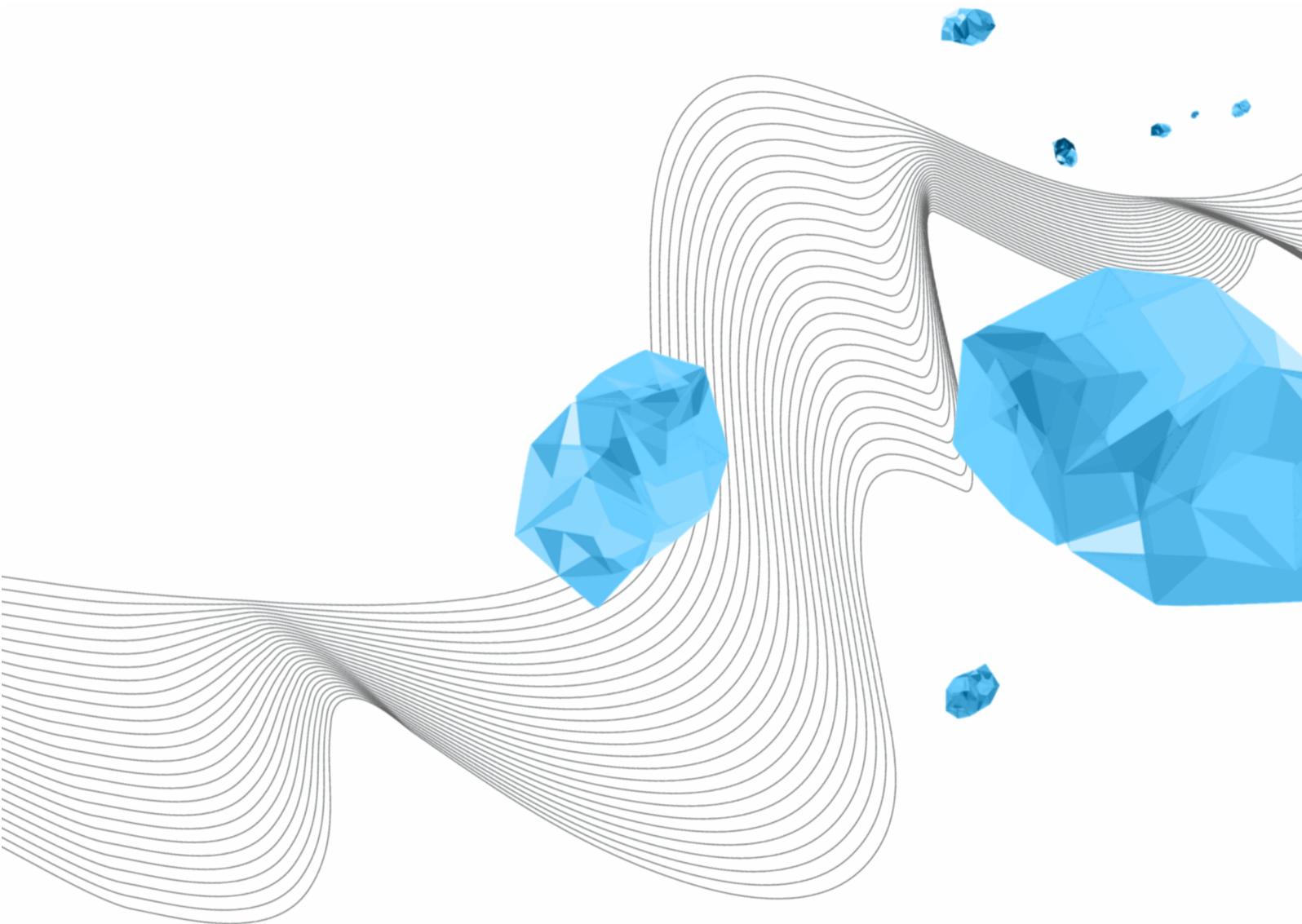


APPROPRIATE USE OF PERSONAL DATA IN SCIENTIFIC RESEARCH ACCORDING TO THE GDPR

FLOW CHART AND PRACTICAL GUIDANCE

Version 1
13-12-2021



COLOPHON

DATE
19-11-2021

VERSION
Version 1

AUTHOR(S)
Maria Kamp (ET)
Lyan Kamphuis-Blikman (BMS)
Marga Koelen (ITC)
Nicole Koster (TNW)
Meike van de Ven-Davids (LISA)
Petri de Willigen (EEMCS)

E-MAIL
dpo@utwente.nl

POSTAL ADDRESS
Mailbox 217
7500 AE Enschede

WEBSITE
www.utwente.nl/privacy

COPYRIGHT
© University of Twente, the Netherlands.

All rights reserved. No part of this publication may be reproduced, stored in an automated data file, or published, in any form or by any means, should it be electronic, mechanical, by photocopies, recordings or any other means, without prior written approval from the University of Twente.



APPROPRIATE USE OF PERSONAL DATA IN SCIENTIFIC RESEARCH
ACCORDING TO THE GDPR by the University of Twente is licensed under a
Creative Commons Attribution 4.0 International License. The full text of the license
can be found at <http://creativecommons.org/licenses/by/4.0/>.

TABLE OF CONTENTS

Appropriate use of personal data in scientific research according to the GDPR	4	
1	Flow chart personal data in research	5
2	Explanation flow chart	6
A.	Do you process personal data in your research?	6
B.	Have you clearly described the purpose for which you process personal data?	6
C.	Is it necessary to process all these personal data in the context of the research and is there a clear retention period?	6
D.	Is personal data used for further processing?	6
E.	Is the processing operation based on consent of the data subject ? Do you meet the conditions the GDPR sets for consent?	7
F.	Can you base the processing operation on another legal basis?	7
G.	Do you collect and/or process special categories of personal data and/or personal data relating to criminal convictions and offences?	7
H.	Have the data subjects been clearly and specifically informed about the processing of their personal data for the research in accordance with the requirements of the GDPR?	8
I.	Do you provide personal data to third parties in the context of the research or do you engage third parties who process personal data on your behalf (or on behalf of the UT)?	8
J.	Other obligations under the GDPR	8
3	Further processing	9
	Compatibility of the purposes of primary and further processing	10
	Appropriate safeguards to protect the privacy of data subjects	10
4	Special categories of and/or criminal personal data	11
	Public interest of the research project	11
	Consent or exemption	11
5	Informing data subjects	13
6	Providing personal data to third parties and engaging processors	14
	Providing personal data to third parties and engaging processors	14

APPROPRIATE USE OF PERSONAL DATA IN SCIENTIFIC RESEARCH ACCORDING TO THE GDPR

When conducting scientific research, personal data may be processed. This can, for example, be data from persons who complete surveys or participate in a research, but it can also be data from social media or tracking data. This document is intended to help researchers determine what they should pay attention to under the General Data Protection Regulation (GDPR).

Scientific research

This document is intended for the use of personal data in scientific research. Under the GDPR, the term 'scientific research' must be broadly interpreted and also includes privately funded research.

However, the research project must meet specific conditions in order to be classified as 'scientific research'. One of these conditions is that the research project must serve a general public interest, is set up in accordance with the relevant methodological and ethical standards and in accordance with good practice. In that context, the research project must meet scientific requirements with regard to publishing or otherwise making (personal) data public for scientific research purposes.

Disclaimer and advice

This document has been prepared by the Data Protection Officer (DPO) of the University of Twente (UT) and the Privacy Contact Persons (PCPs) of the faculties of the UT with the help of an external privacy lawyer.

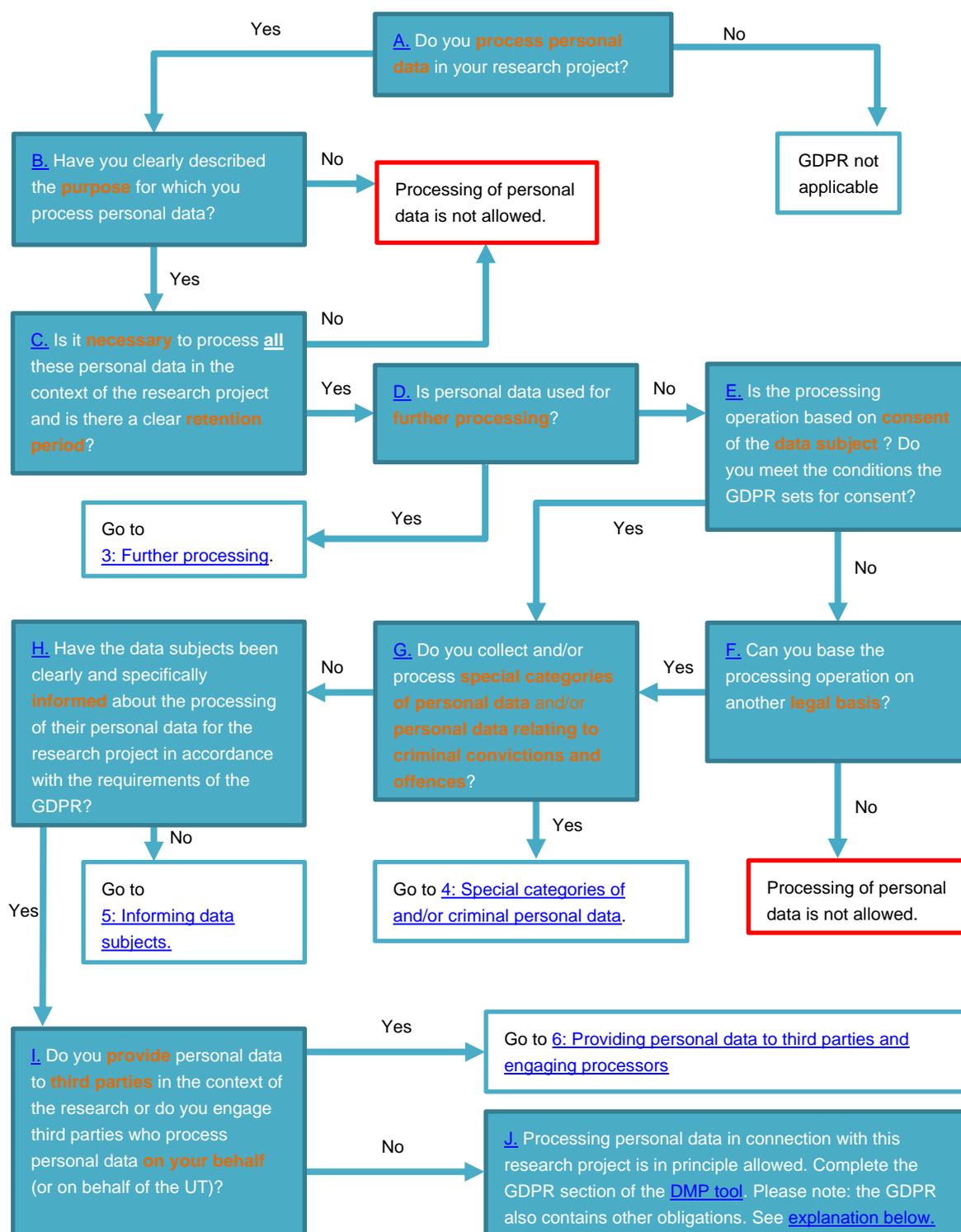
This document is not exhaustive. Some items may also be formulated differently and/or have been limited or not included in this document for the sake of clarity and readability. Therefore, some nuances may have been omitted.

This document is prepared as a tool to help you. You cannot derive any rights from this document. In case you process personal data within your research, you must register this processing operation in the [GDPR register](#). You can always ask the [PCP of your faculty or the DPO](#) for advice.

Lastly, this document only handles the GDPR aspects of scientific research. In case you process personal data within your research, you must also ask for an ethical review. You can find more information on [this website](#).

1 FLOW CHART PERSONAL DATA IN RESEARCH

You can find an explanation of the questions and the terms **in bold** in [2: Explanation flow chart](#). Most definitions can also be found on [this page](#).



2 EXPLANATION FLOW CHART

The explanations correspond to the letters included in the boxes in the flow chart.

A. Do you process personal data in your research project?

Personal data means: any information relating to an identified or identifiable natural person (the **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.

Researchers regularly use **anonymous or pseudonymised data**. **Anonymous data** are not related to an identified or identifiable person, or are anonymised in a way that a person is no longer identifiable. The GDPR does not apply to anonymous data. **Pseudonymized data** are data that are processed in a way that they can no longer be linked to a specific data subject, without using additional data. Pseudonymized data are personal data under the GDPR. Therefore, the GDPR does apply to pseudonymized data. In most cases in research, pseudonymized data are involved instead of anonymized data.

Everything that can be done with personal data is called **processing**, for example collecting, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

B. Have you clearly described the purpose for which you process personal data?

It is important to determine the **purposes** for processing personal data prior to that processing: what are you researching? What is your research question and how do you wish to investigate this with the required personal data? If it is impossible to accurately describe the purposes for processing personal data in advance, you may, by exception, describe the purposes at a more general level. Personal data may not be further processed in a manner incompatible with those purposes.

C. Is it necessary to process all these personal data in the context of the research project and is there a clear retention period?

Make sure you do not process any personal data that is not **necessary** for conducting the research. Make sure you can explain why processing certain personal data is necessary for the research project. You may not process more personal data than necessary for the purpose of that processing (the principle of **data minimisation**). The retention period of the personal data must be kept to a strict minimum. You must therefore determine a **retention period** and after that period, the personal data must be deleted. In the case of scientific research, the retention period will often be 10 years; after this period, personal data must be deleted. This term is in line with the term in the RDM policy.

D. Is personal data used for further processing?

Scientific research with personal data can be conducted in two ways:

1. **Primary processing**: You collect (personal) data yourself and you use this data to conduct research. In this situation, the main rule applies: you must have a legitimate purpose and a legal basis for the processing of personal data.

2. **Further processing:** You conduct research into and/or with use of data that has already been collected by the UT at an earlier stage for another purpose. In that case, it is called further processing. If certain requirements are met, a legal basis may not be required. See [3: Further processing](#) for these requirements.

E. Is the processing operation based on consent of the data subject ? Do you meet the conditions the GDPR sets for consent?

The processing of personal data must be based on a **legal basis**. In principle, you can use the legal basis “**consent** of the data subject”. You must meet the conditions the GDPR sets for consent:

1. Is the consent a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her?
 - **Freely given:** the data subject may not be pressured to consent. If the data subject does not consent, this may not have any consequences. You should also pay attention to power relations, for example employer – employee. In such situations, it may be more difficult to construct freely given consent.
 - **Specific:** consent must be given for a specific processing operation and for a specific purpose. In case you will process personal data for multiple purposes, you must ask for consent for each of those purposes.
 - **Informed:** data subjects must be informed about the identity of the organisation, the purpose of the processing operation for which consent is asked, what personal data will be processed and the possibility for the data subject to withdraw his or her consent. This information must be given in clear and simple language.
 - **Unambiguous:** consent must be given by a clear, active action. It is not allowed to use pre-ticked boxes.
2. Have you informed the data subject that he/she can always withdraw his/her consent? [Here](#), you can read what you should do if a data subject withdraws his/her consent (the question: ‘Can a participant in scientific research withdraw his/her consent to process his/her personal data?’).
3. Can you demonstrate that you have obtained consent? Has this been documented?

F. Can you base the processing operation on another legal basis?

Can you base the processing operation on a **legal basis**? Personal data may only be processed **lawfully** and that is only the case if the processing operation can be based on at least one of the legal bases. The GDPR lists six legal bases; click [here](#) for more information. Not all six legal bases are relevant for scientific research.

If it is not possible to ask data subjects for consent, the ‘public interest’ basis may be invoked. In that event, the processing operation is necessary to fulfil a *public task* assigned to the UT. In certain situations, research can meet specific characteristics of scientific research. Under the Higher Education and Scientific Research Act, the UT has the task of conducting scientific research. If you can justify that it is necessary to process personal data in order to fulfil this task, you can base your processing operation on this legal basis.

Please note: under the GDPR, in some cases, you can further process the personal data for purposes other than those for which the personal data was originally collected. In those events, no separate legal basis is required. See [3: Further processing](#).

G. Do you collect and/or process special categories of personal data and/or personal data relating to criminal convictions and offences?

Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

Personal data relating to criminal convictions and offences also include related security measures.

Processing special categories of personal data and personal data relating to criminal convictions and offences is prohibited by the GDPR if certain conditions are not met. Processing someone's **social security number** is prohibited, unless otherwise stated in the law.

Please note: special categories of personal data can also relate to someone's online behaviour, for example responding or likes on social media; even when it is public. For example, this may involve someone's political views or religious or philosophical beliefs.

See [4: Special categories of and/or criminal personal data](#).

H. Have the data subjects been clearly and specifically informed about the processing of their personal data for the research project in accordance with the requirements of the GDPR?

The data subjects can, for example, be **informed** about the processing of their personal data by means of a privacy statement on a website or via information leaflets. You must inform data subjects prior to processing their data. For example, you can inform respondents about the processing prior to their participation. The GDPR states what information must be provided to the data subjects. See [5: Informing data subjects](#).

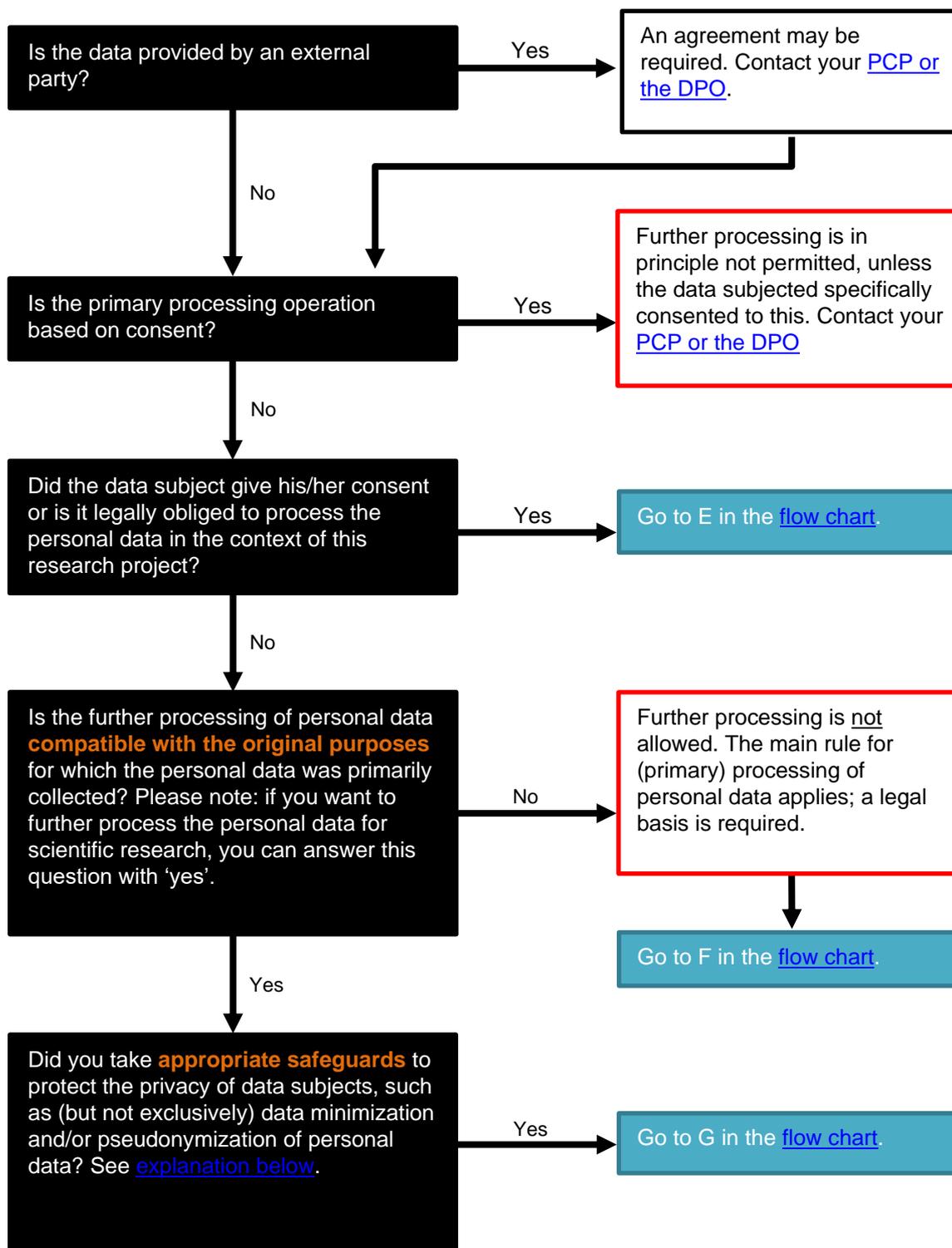
I. Do you provide personal data to third parties in the context of the research project or do you engage third parties who process personal data on your behalf (or on behalf of the UT)?

Consider, for example, the **transfer** of personal data to external collaboration or research partners, or the possibility that such external parties have access to personal data processed by you in the context of the research project. It is also possible to engage third parties who will process personal data **on behalf of the UT** in the context of the research project, such as external hosting parties that store research data – containing personal data – on their servers. See [6: Providing personal data to third parties and engaging processors](#).

J. Other obligations under the GDPR

The GDPR has various other obligations relating to processing personal data. Given the scope of this document, not all of these obligations are covered here. Some examples of these obligations are obligations with regard to the security of personal data, data breaches and carrying out a DPIA. The [pre-DPIA](#) helps you to assess whether a DPIA is necessary. Furthermore, the data subjects have various [rights](#) under the GDPR.

3 FURTHER PROCESSING



Compatibility of the purposes of primary and further processing

If personal data are further processed in scientific research, the purposes of that further processing operation must be **compatible with the purposes** of the primary processing operation.

To determine whether in other cases further processing of **personal data is compatible with the purposes for which the personal data was originally collected**, the following questions should be considered:

- What is the connection between the purposes for which the personal data were primarily collected and the purposes of the intended further processing operation?
- What is the framework in which the personal data are collected, in particular with regard to the relationship between the data subjects and the UT?
- What is the nature of the personal data? For example, do you process special categories and/or criminal personal data or social security numbers?
- What are the possible consequences of the intended further processing for data subjects?
- Has the UT taken [appropriate safeguards](#), including possible encryption or pseudonymization?

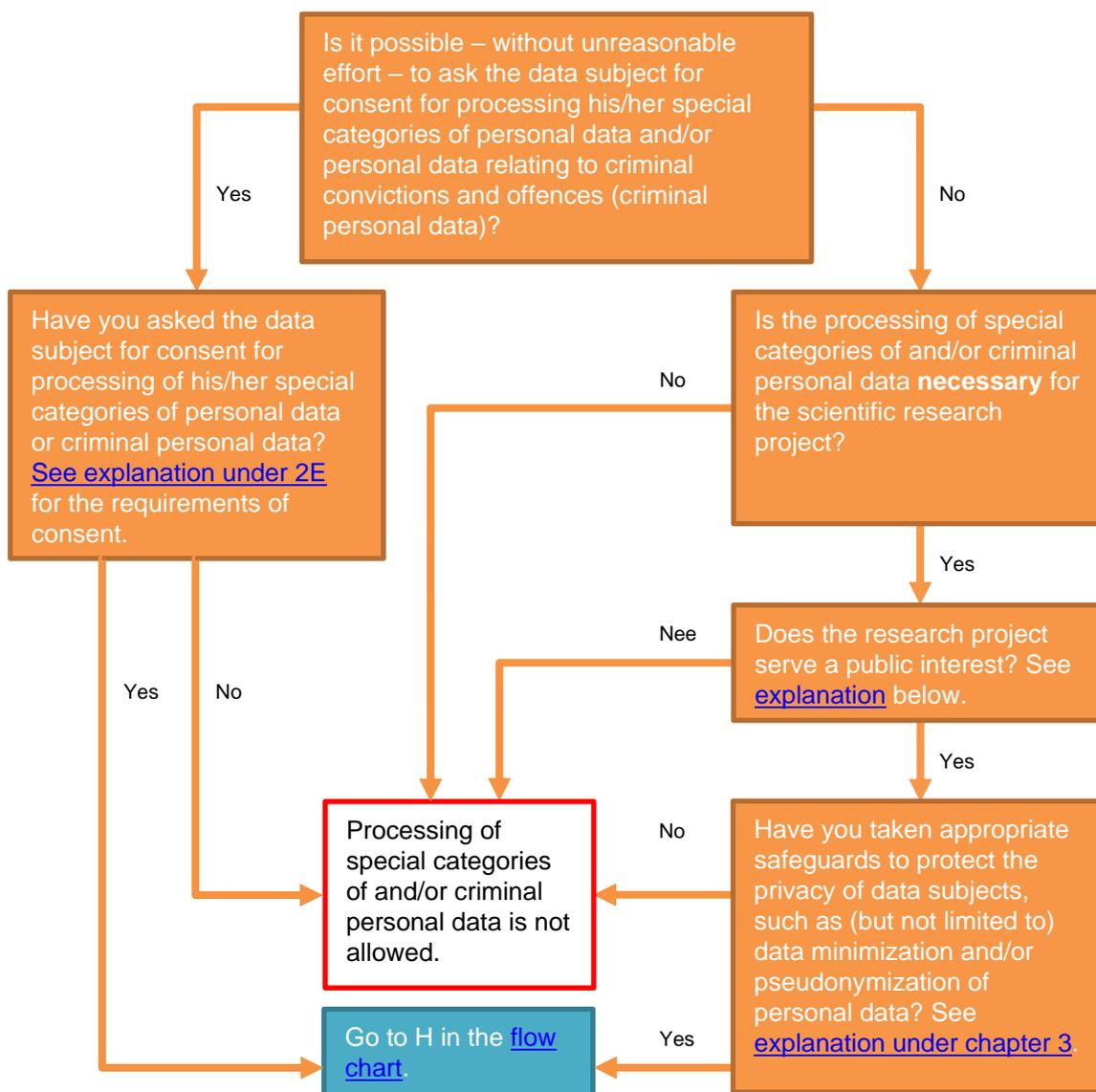
Your [PCP](#) can help you with this assessment.

Appropriate safeguards to protect the privacy of data subjects

Examples of **appropriate safeguards** are:

- Encrypting personal data;
- Pseudonymizing – or even anonymizing – personal data;
- Measures regarding access to and confidentiality of personal data;
- Measures regarding the presentation of the results of the research project;
- Measures to process as little personal data as possible; do not process more personal data than strictly necessary for the purposes of processing (data minimization).

4 SPECIAL CATEGORIES OF AND/OR CRIMINAL PERSONAL DATA



Public interest of the research project

The research project serves a 'public interest' if the purpose of the research project entails that a substantial group can benefit from it. In medical research projects, this could for example be the promotion or protection of public health. Studies that are only conducted in connection with an industrial or commercial interest, do not meet the 'public interest' criterion. In those event, you cannot base your processing operation on this exemption.

Consent or exemption

If you want to process special categories of and/or criminal personal data for scientific research, you must ask data subjects for consent. See the explanation on consent under [2 E: Is the](#)

[processing operation based on consent of the data subject ? Do you meet the conditions the GDPR sets for consent?](#)

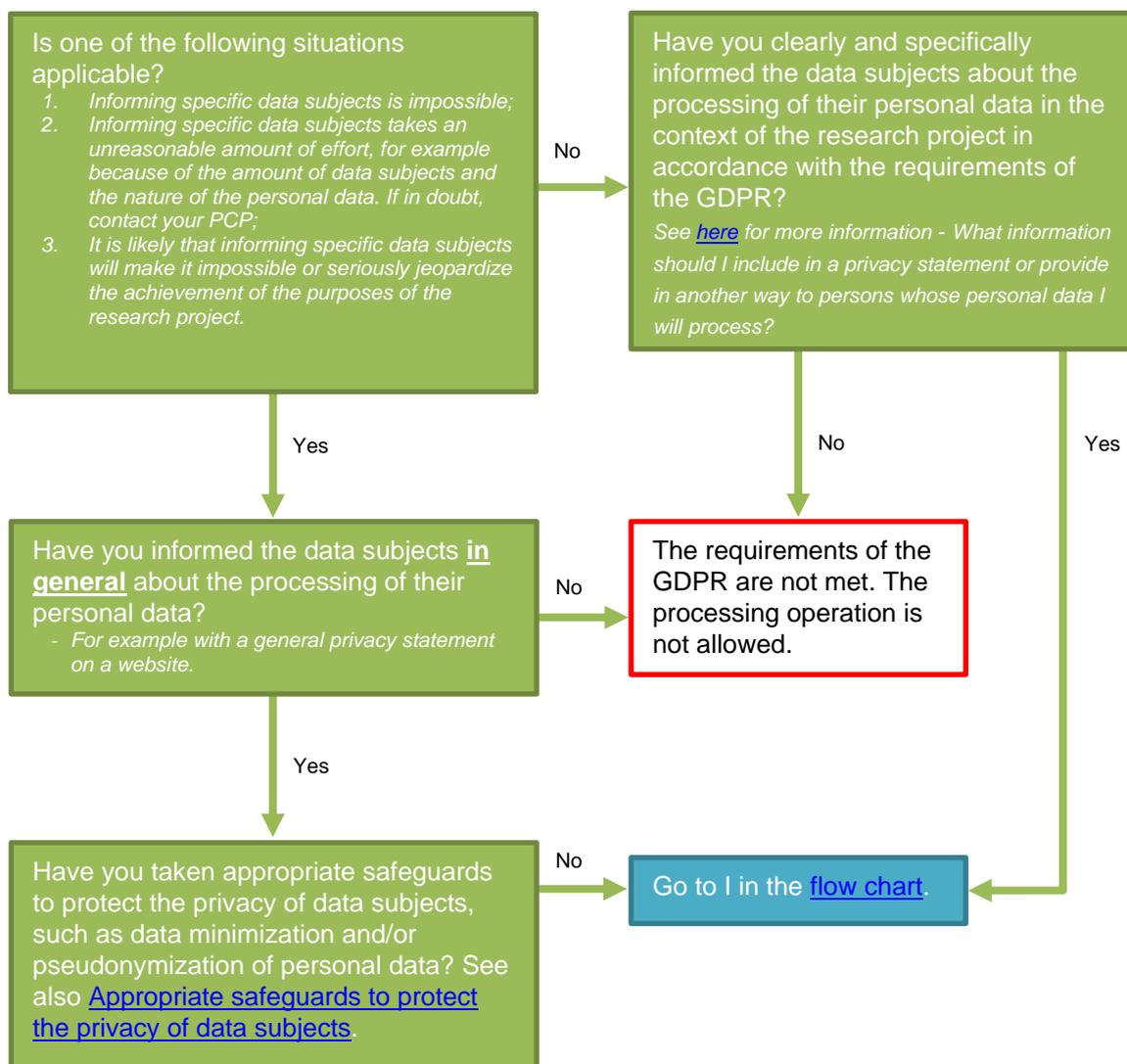
Only if you can demonstrate with reasons that it is impossible to ask the data subject for consent, the processing of special categories of and/or criminal personal data may be permitted if all of the following conditions are met:

- a. the research project must serve a [public interest](#);
- b. the processing of personal data must be necessary for the research project;
- c. asking for explicit consent must be impossible or entails an unreasonable effort; and
- d. appropriate safeguards must be in place to ensure that the privacy of the data subjects is not disproportionately harmed.

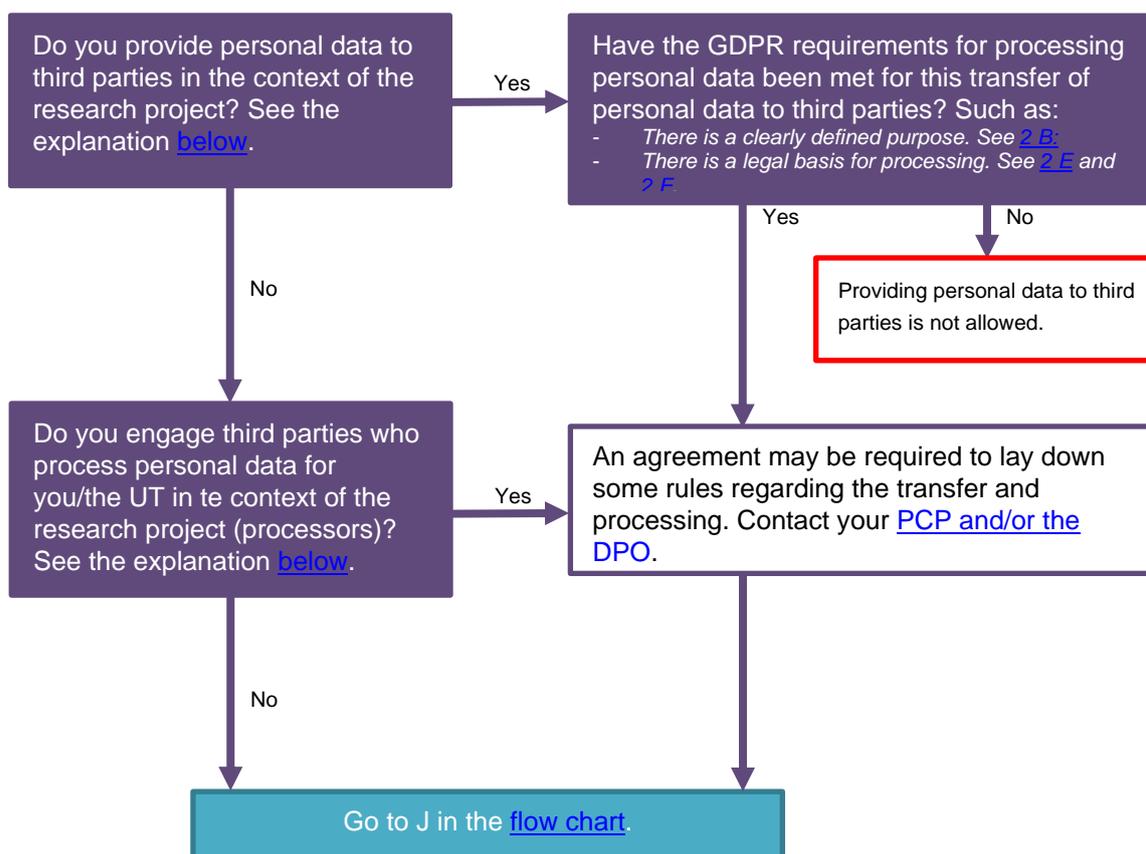
Contact your [PCP or the DPO](#) to help you with assessing these conditions.

Please note: in case an exemption is applicable for the processing of special categories of and/or criminal personal data, this is only a first step: the processing operation must also be lawful on the basis of the general conditions of the GDPR, such as having a legitimate purpose and a legal basis. See [2 B: Have you clearly described the purpose for which you process personal data?](#) and [2 F: Can you base the processing operation on another legal basis?](#)

5 INFORMING DATA SUBJECTS



6 PROVIDING PERSONAL DATA TO THIRD PARTIES AND ENGAGING PROCESSORS



Providing personal data to third parties and engaging processors

For example:

- the transfer of personal data to external collaboration or research partners in the context of the research project.
- the possibility that such external parties have access to the personal data processed by you in the context of the research project. Since the provision of personal data to third parties is a way of processing personal data, the previous steps in the [flow chart](#) must be reconsidered.
- Engaging external parties who will process personal data on behalf of you/the UT in the context of the research project, such as external hosting parties that store research material – containing personal data – on their servers.