Annex - Legitimate Interest Assessment (LIA) flowchart

on the three-steps test methodology

Preliminary considerations

The Legitimate Interest Assessment (LIA)
must be carried out before the relevant processing begins.

Before proceeding with the three-step test, check the following:

1. Have you identified the specific processing activity, its purpose, the means and circumstances of the processing?

2. Have you checked that Union or Member State law does not require another legal basis or preclude reliance on legitimate interests?

If yes, proceed with the three-step test.

STEP 1

The pursuit of a legitimate interest test (paras. 13-24)

Does the identified interest qualify as a legitimate interest for the purposes of Article 6(1)(f) GDPR?

Identify and describe the interest pursued

Identify the interest, including its nature, source and weight.

Identify whose interest is pursued: your own interest, the interest of a specific third party or parties, and whether these interests correspond or coincide with a wider public interest.

Identify the expected benefits of the processing, and whether these are benefits for your organisation, third parties or/and the wider public.

Check whether the interest is: (para. 16)

- lawful;
- clearly articulated;
- present and effective;

STEP 2

Necessity test (paras. 25-27)

Is the processing necessary to pursue the identified legitimate interest?

Can the identified legitimate interest be reasonably achieved just as effectively through less intrusive means? (para. 26)

In assessing this, consider whether the processing is adequate, relevant and limited to what is necessary for the purpose pursued, in line with Article 5(1)(c) GDPR.

Inter alia, ask yourself:

- Is the processing of personal data in question suitable and relevant to actually achieve the purpose and pursue the identified legitimate interest?
- Can the scope or amount of personal data processed be reduced?
- Can the number of data subjects be limited to the minimum necessary to achieve the purpose?
- Can the duration or frequency of the processing be limited, for example by carrying it out on a one-off rather than an ongoing basis?

STEP 3

Balancing test (paras. 28-58)

Do the data subject's interests, rights and freedoms override the identified legitimate interest?

How does the processing affect data subject's interests, fundamental rights and freedoms? (paras. 31-34)

Check how and to which extent the processing may affect the data subject's fundamental rights and freedoms, including the rights to data protection and privacy, as well as any other relevant fundamental rights and freedoms.

Check whether the processing may affect any other interests of the data subject, such as financial, social or personal interests.

Identify and describe the impact of the processing on the data subject, including the nature of the data, the context and further consequences of the processing. (para. 35)

Nature of the data processed (paras. 36-38)
Does the processing involve any of the following?

- special category data or criminal convictions/offences data (Art. 9, 10 GDPR);
- data likely to be considered particularly "private" (such as financial data or location data);
- Is the data rather of a more public nature (e.g. data concerning the data subject's professional role)?

Context of the processing (paras. 39-40)

What is the scale of the processing and the amount of personal data to be processed?

Is there an established relationship with the data subject and if so, what is the nature of the relationship?

Will the personal data to be processed be combined with other data sets?

How accessible / publicly available is the data to be processed?

What is the status of the data subject (e.g. children, vulnerable individuals)?

Measures limiting the impact

Which technical, organisational or other measures have been implemented to limit the impact of the processing on the data subject, including in light of Articles 5(1)(c) and 25 GDPR? (para. 45)

Further consequences (paras. 41-46)

What are the possible further consequences of the processing for the data subject, whether positive or negative?

Consider benefits for the data subject, as well as possible risks such as financial loss, reputational harm, discrimination, loss of privacy or control, emotional distress, chilling effects, or legal or similarly significant effects such as refusal of credit, job rejection or service denial.

Would the data subject reasonably expect their data to be processed in this way? (paras. 47-51)

Consider what can justifiably be expected in the specific context of the processing, taking into account among other factors: (para. 51)

- the existence and nature of the relationship with the data subject;
- the nature and characteristics of the service;
- the place and context of the data collection;
- any applicable legal or sector-specific requirements;
- the characteristics of the (average) data subject (e.g. minors, public figures, professionals);
- the transparency of the processing and information provided.

Final balancing outcome (paras. 52-58)

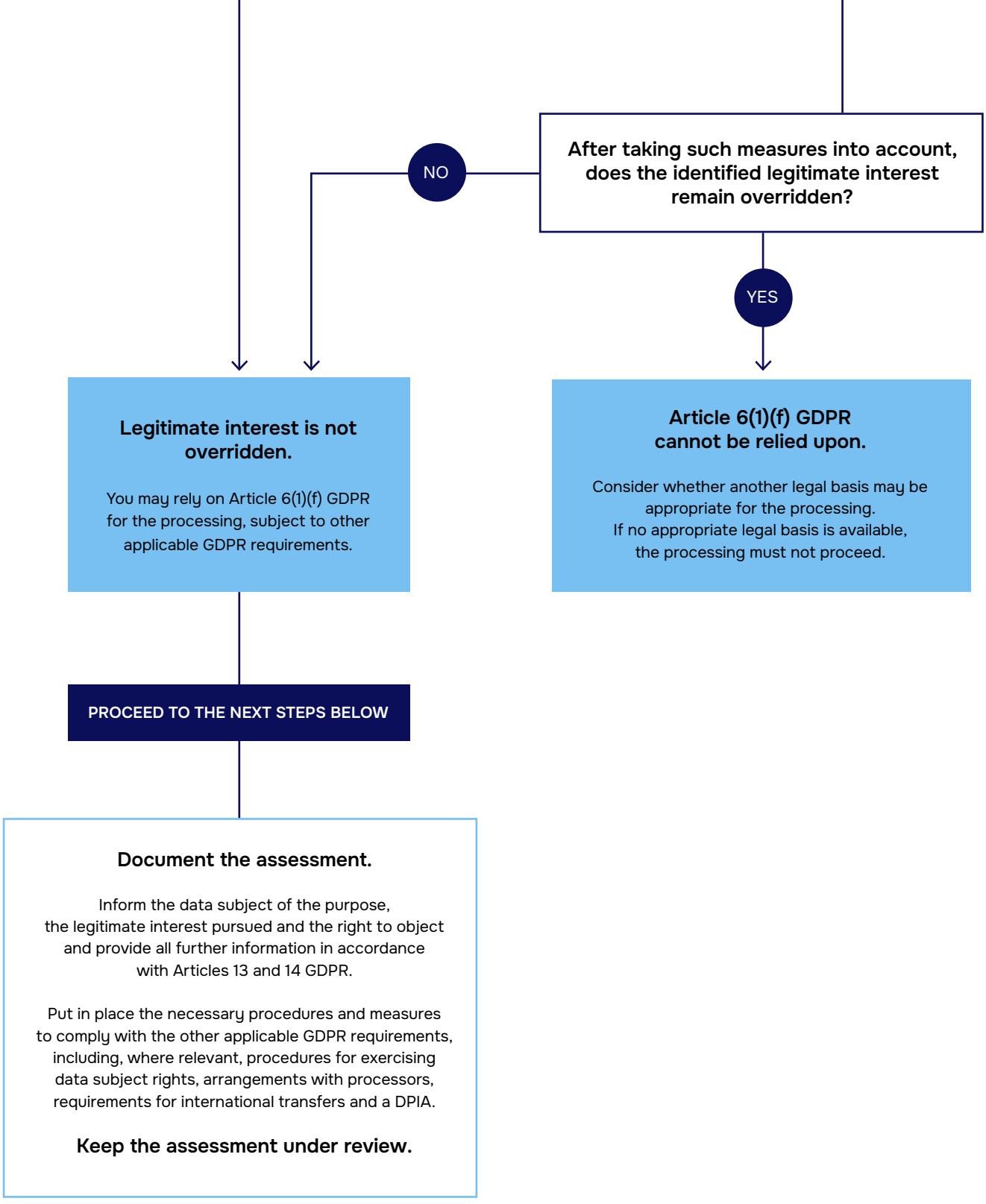
Taking into account the weight of the identified legitimate interest, the relevant interests, rights and freedoms of the data subject, the impact of the processing on the data subject and the data subjects' reasonable expectations, is the identified legitimate interest overridden by the data subjects' interests, rights and freedoms?

YES

Additional mitigating measures

If the identified legitimate interest is overridden, consider additional measures to limit the impact on the data subject, such as an unconditional opt-out (paras. 53-54).
Where such measures are adopted, document how they change the outcome of the balancing test and determine whether the identified legitimate interest remains overridden. (para. 56)

NO


After taking such measures into account, does the identified legitimate interest remain overridden?
NO
YES
Legitimate interest is not overridden.
You may rely on Article 6(1)(f) GDPR for the processing, subject to other applicable GDPR requirements.
Article 6(1)(f) GDPR cannot be relied upon.
Consider whether another legal basis may be appropriate for the processing. If no appropriate legal basis is available, the processing must not proceed.
PROCEED TO THE NEXT STEPS BELOW
Document the assessment.
Inform the data subject of the purpose, the legitimate interest pursued and the right to object and provide all further information in accordance with Articles 13 and 14 GDPR.
Put in place the necessary procedures and measures to comply with the other applicable GDPR requirements, including, where relevant, procedures for exercising data subject rights, arrangements with processors, requirements for international transfers and a DPIA.
Keep the assessment under review.