GDPR

Legitimate interests

What's new?

What is the legitimate interests basis?

When can we rely on legitimate interests?

How do we apply legitimate interests?

The key elements of legitimate interests are the same, but…

…there are some changes to the detail

Legitimate interests are no longer limited to your own interests or those of third parties to whom you disclose data

You can now consider the interests of any third party, including the wider benefits to society

Legitimate interests is not just a pure harm-based assessment

For example an individual's rights may override legitimate interests if they don't reasonably expect the processing

You have new accountability and transparency requirements

You need to:

- Document your assessment of how legitimate interests applies
- Tell individuals what your legitimate interests are

The GDPR also specifically highlights children's data as needing special consideration

What's new?

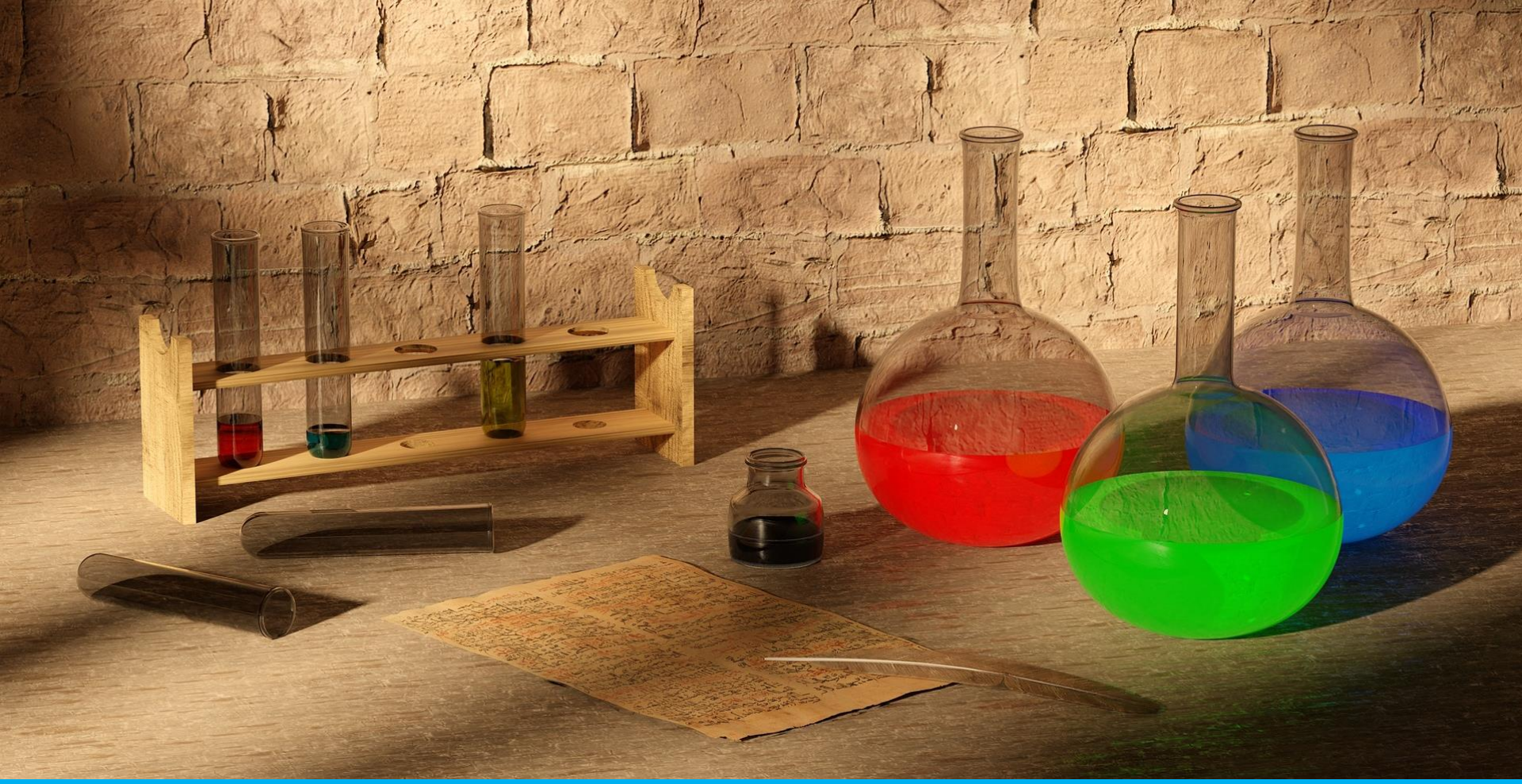
What is the legitimate interests basis?

When can we rely on legitimate interests?

How do we apply legitimate interests?

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

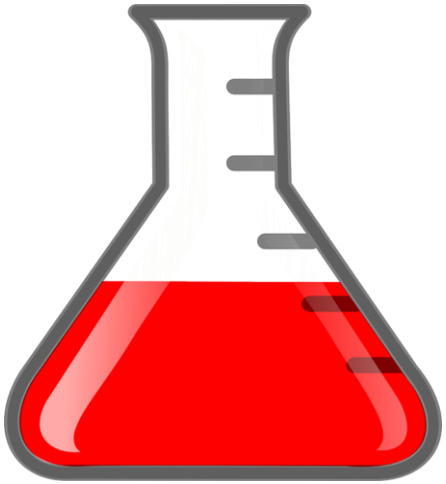
Article 6(1)(f) Legitimate interests



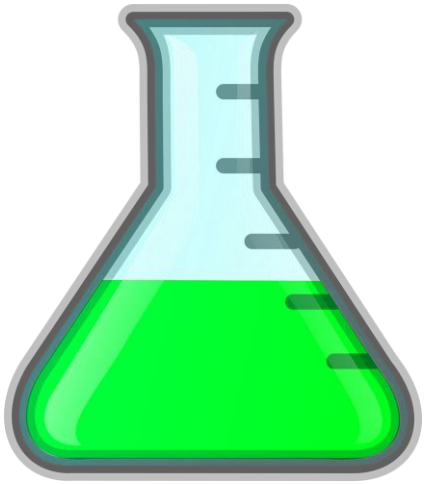
The legitimate interests provision can be broken down into a three-part test

What is the three-part test?

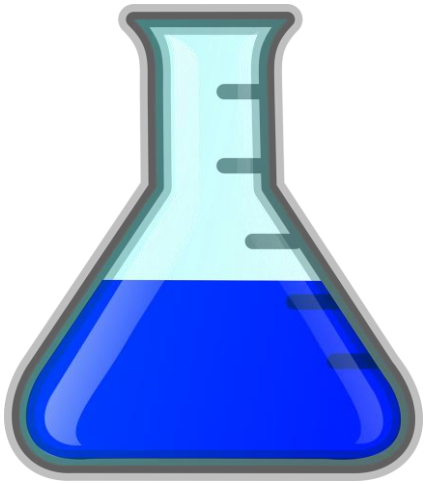
1
Purpose test
Are you pursuing a legitimate interest?



2
Necessity test
Is the processing necessary for that purpose?



3
Balancing test
Do the individual's interests override the legitimate interest?



What counts as a legitimate interest?

The ‘legitimate interest’ could be for example:

- your own interests;
- the interests of a third party;
- commercial interests; or
- wider societal interests.

The term ‘legitimate interest’ is broad. The interests could be compelling or in some cases could be more trivial. However you or a third party must have some clear or specific benefit or outcome in mind.

GDPR mentions use of client or employee data, marketing, fraud prevention, intra group transfers, IT security and disclosing information about possible criminal acts or security threats as potential legitimate interests but this is not an exhaustive list

When is processing necessary?

Necessary means the processing must be a targeted and proportionate way of achieving your purpose

If there is another reasonable and less intrusive way to achieve the same result you can't rely on legitimate interests

What is the balancing test?

The balancing test is where you balance your interests against the interests, rights and freedoms of the individual

The interests, rights and freedoms of individuals could cover any type of impact including physical or financial harm, or any social or economic disadvantage

What's new?

What is the legitimate interests basis?

When can we rely on legitimate interests?

How do we apply legitimate interests?

When might legitimate interests be appropriate?

It might be appropriate when:

The processing is not required by law but is of a clear benefit to you or others;

There's a limited privacy impact on the individual;

The individual should reasonably expect you to use their data in that way; or

You can't or don't want to give the individual full upfront control or bother them with disruptive requests.

Can public authorities use legitimate interests?

Yes, in some instances they can

But not if the processing is to perform their tasks as a public authority

Can legitimate interests be used to process children's data?

Yes, the GDPR doesn't prevent you relying on legitimate interests to process children's data

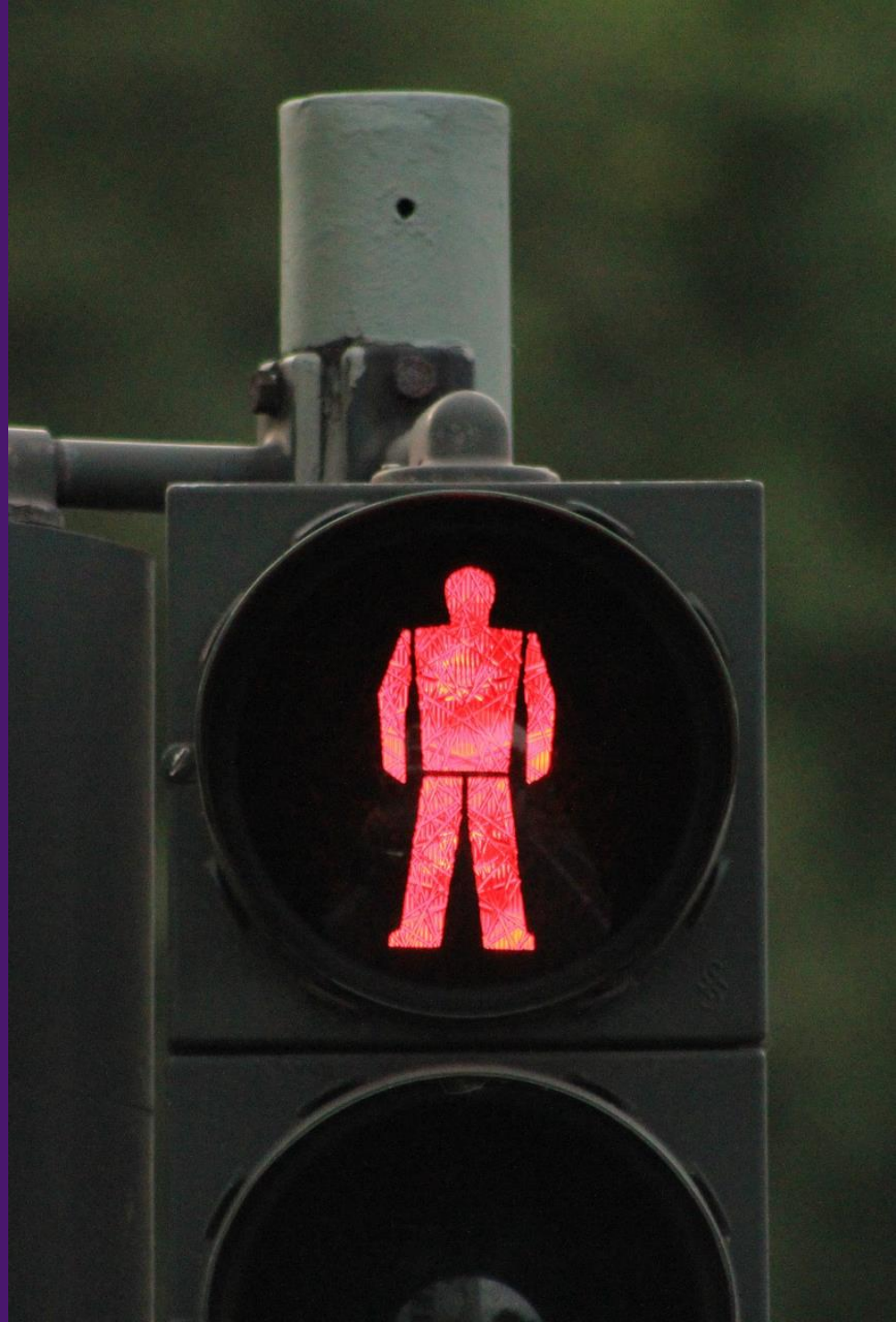
But you have a responsibility to protect them from risks and consequences that they may not fully understand or envisage, and adequately protect their interests

Can we use legitimate interests for direct marketing?

Yes, in some cases

But you will need to apply the three-part test and ensure that you comply with other marketing laws

When might legitimate interests be inappropriate?



For example you should avoid legitimate interests if:

You are a public authority and the processing is to perform your tasks as a public authority;

Your processing does not comply with broader legal, ethical or industry standards;

You don't want to take full responsibility for protecting the interests of the individual or would prefer to put the onus on them; or

You're not confident of the outcome of the balancing test.

What's new?

What is the legitimate interests basis?

When can we rely on legitimate interests?

How do we apply legitimate interests?

Legitimate interests assessment (LIA)

What is an LIA?

This is where you assess each part of the three-part test and record the outcome

We call it a 'legitimate interests assessment' or LIA for short

An LIA is a light-touch risk assessment based on the specific context and circumstances

Do we need to record our LIA?

Yes, you need to record your LIA and the outcome

There's no specific requirement to do this but you are likely to need an audit trail of your decisions and justifications


How do we do the
purpose test

Ask yourself:

Why do you want to process the data?

What benefit do you expect to get from the processing?

Who else benefits from the processing (third parties/the public)?

How important are those benefits?

What would the impact be if you couldn't go ahead?

What is the intended outcome for individuals?

Are you complying with other relevant laws and industry guidelines/codes?

Are there any ethical issues with the processing?

Are you processing for fraud prevention, IT security or any of the purposes highlighted by the GPDR?


How do we do the
necessity test

Ask yourself:

Will the processing actually help you achieve your purpose?

Is the processing proportionate to that purpose?

Can you achieve your purpose without processing the data, or processing less data?

Can you achieve your purpose by processing the data in another more obvious or less intrusive way?


How do we do the
balancing test

As a minimum consider:

The nature of the personal data you want to process;

The reasonable expectations of the individual; and

The likely impact of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

Nature of the personal data

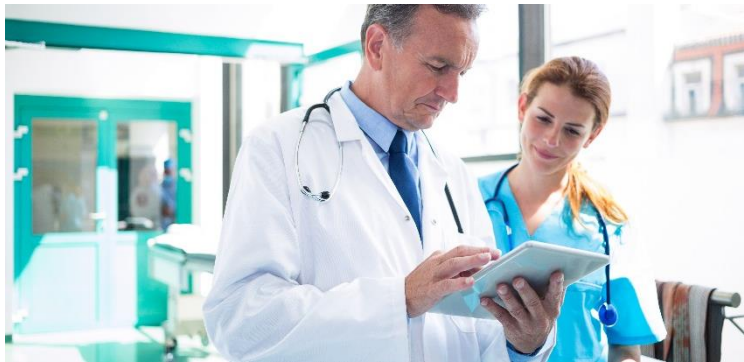
You need to think about the sensitivity of the personal data

For example is it:

- special category data?
- criminal offence data?
- children's data?
- data about personal or professional life?

Nature of the data

The more sensitive or 'private' the data the more likely the processing will be considered intrusive or create significant risks to the individual's rights and freedoms



Reasonable expectations

You need to think what people would reasonably expect you to do with their data in the particular circumstances

For example :

- what is the nature of your relationship with them?
- did the data come directly from them?
- is your intended purpose widely understood?

Reasonable expectations

This is an objective test – you don't have to show that every individual expects you to use their data in this way. Instead you have to show that a reasonable person would expect it.

Impact and safeguards

You need to consider the potential impact on individuals and any damage the processing might cause them

For example could the processing lead to:

- difficulty in exercising rights?
- physical harm?
- financial loss or identify fraud?

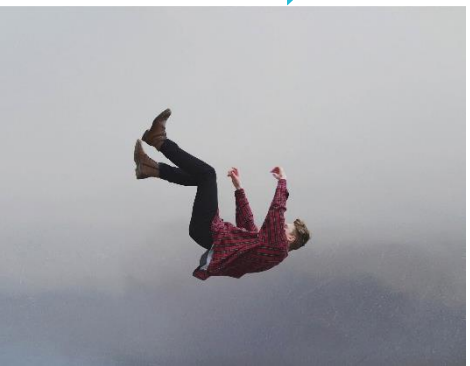
Impact and safeguards

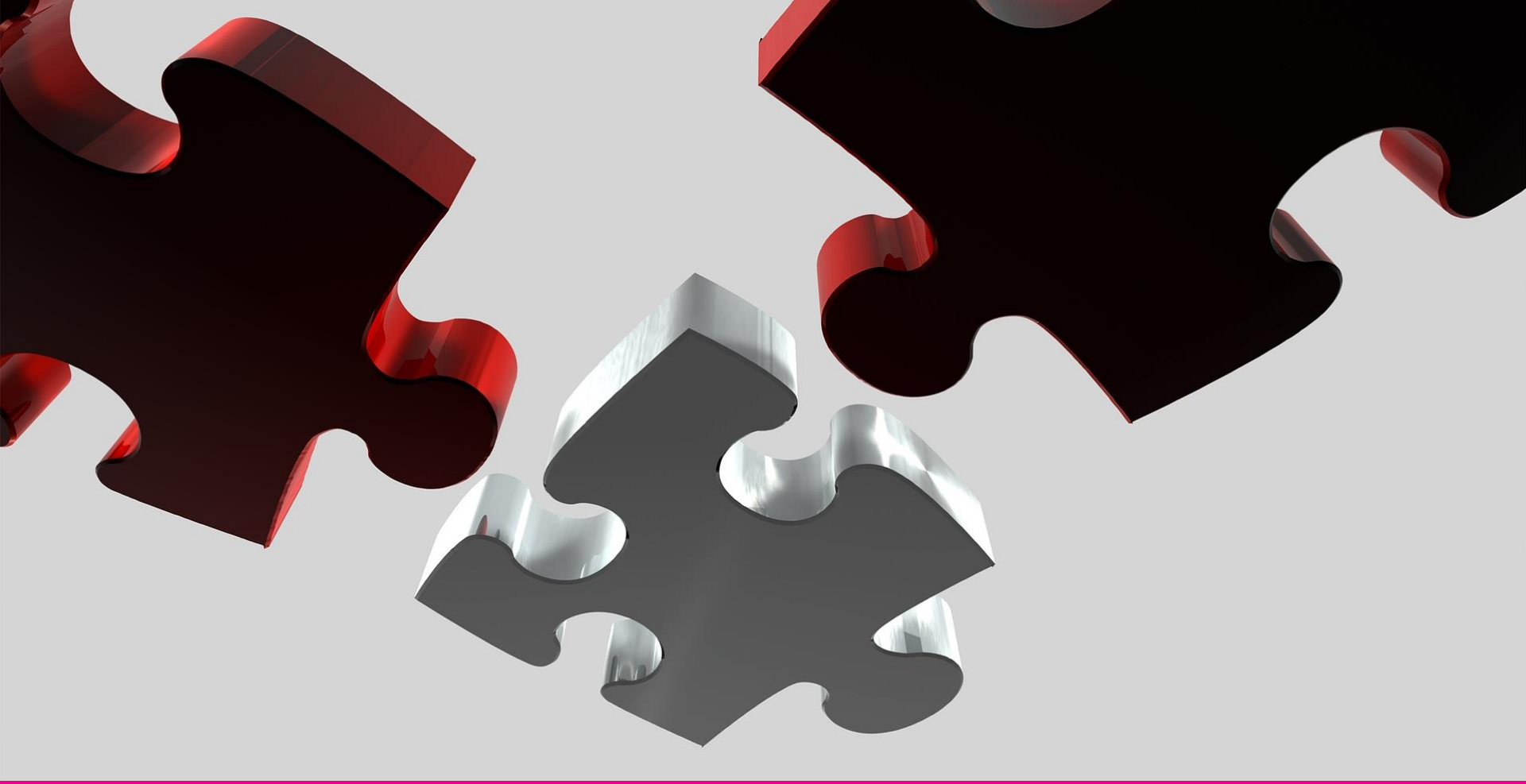
If you identify potential for high risk you need a much more compelling legitimate interest to satisfy the balancing test. You also may need to conduct a DPIA.

Impact and safeguards

You may want to consider if there are any safeguards you can build in to reduce or mitigate the risk

Appropriate safeguards can change the balance and mean that the individual's interests no longer override yours, but this will not always be possible





Deciding the outcome of an LIA

You need to weigh up all the factors that you identified during your LIA for and against the processing

You should be as objective as possible when deciding whether you think your interests take priority over any risk to individuals

Sometimes the outcome will very obviously weigh in one direction

Sometimes it may be harder to decide

If you're not sure it might be safer to see if another basis applies

More information is available...

Pick up a leaflet from the hub

Check out our lawful basis tool

Visit our website www.ico.org.uk

This slideshow will restart shortly

Subscribe to our e-newsletter at www.ico.org.uk
or find us on…

@iconews