1. Territorial scope fundamentals

Territorial scope of the UK GDPR

What's the territorial scope of the UK GDPR?

The UK GDPR applies in three specific situations:

- **Establishment:** if an organisation has an establishment inside the UK. The UK GDPR applies to processing linked to the activities of that establishment – even if the processing itself takes place outside the UK. See What's an establishment?

- **Targeting:** if an organisation isn't established in the UK, but offers goods or services to people in the UK, or monitors the behaviour of people in the UK. The UK GDPR applies to processing related to that targeting activity. See What does targeting mean?

- **Public international law:** if an organisation is outside the UK, but established in a place where UK law applies (eg in a consulate or embassy, or a cruise ship registered in the UK).

If none of these apply, the UK GDPR doesn't apply. In such cases, we don't have any jurisdiction and can't take action.

If it's not clear, it's likely the UK GDPR doesn't apply. There's a general presumption that domestic laws won't apply overseas, unless there's a clear legal provision with clear justification.

And bear in mind that UK law won't apply to overseas government bodies - see for example the Clearview case summary.[1]

For these purposes, the UK means England, Northern Ireland, Scotland and Wales. It doesn't include Crown dependencies or UK overseas territories. For example, this means that it doesn't include the Channel Islands, the Isle of

Man or Gibraltar - they have their own data protection laws. See also: What are British Overseas Territories and how does DP law apply? and Does UK DP law apply in the Isle of Man or the Channel Islands?

Territorial scope of the DPA 2018

What's the territorial scope of the Data Protection Act 2018?

Part 2 of the DPA 2018 applies where the UK GDPR applies. See What's the territorial scope of the UK GDPR?

Part 3 of the DPA 2018 (the law enforcement regime) only applies if the controller is a UK law enforcement authority, and the handling of data is linked to the activities of an establishment in the UK. It doesn't matter if the data itself is actually handled outside the UK.

Similarly, Part 4 of the DPA 2018 (the intelligence services regime) only applies if the controller is one of the UK intelligence services, and the handling of data is linked to the activities of a UK establishment. Again, it doesn't matter if the data itself is actually handled outside the UK.

For these purposes, the UK means England, Northern Ireland, Scotland and Wales. It doesn't include Crown dependencies or UK overseas territories. For example, this means that it doesn't include the Channel Islands, the Isle of Man or Gibraltar – they have their own data protection laws. See Crown dependencies and British Overseas Territories.

Territorial scope and controllers

How does territorial scope apply to controllers?

You need to remember the following points:

- Look at each processing activity (collection, storage or use of data) on its own merits, rather than the organisation as a whole.
- If the controller has a UK establishment, the UK regime will apply to any handling of data with an inextricable link to that establishment's activities.
- If the controller doesn't have a UK establishment, but is actively offering services into the UK or monitoring people in the UK, then the UK regime will apply to related handling of data.
- The UK regime won't apply to a controller outside the UK just because it uses a UK processor.
- The UK regime won't automatically apply to a joint controller outside the UK just because it's working with a joint controller inside the UK (or with a joint controller who is targeting the UK). The UK regime is likely to apply in some cases, but this will depend on the facts. You need to look at the specific processing activity (collection, storage or use of data), and find a specific link to the activities of the other joint controller's UK establishment (or to its UK targeting activities).

Territorial scope and processors

How does territorial scope apply to processors?

You need to remember the following key points:

- Look at each processing activity (collection, storage or use of data) on its own merits, rather than the organisation as a whole.
- If a processor has a UK establishment, then the UK regime will apply to any handling of data linked to the establishment's activities. Only the direct processor obligations will apply - you should consider the controller separately.

- If the processor doesn’t have a UK establishment, you should then ask whether the controller has a UK establishment, or is actively targeting people in the UK by offering services into the UK or monitoring people in the UK. If so, you ask whether the handling of data has a clear and specific link to that UK activity. The UK regime will only apply to any handling of data with an inextricable link to the activities of the UK establishment, or directly related to the targeting activity - but this may include data-handling carried out by the processor acting on the controller’s behalf.

- A non-UK processor won't be automatically covered just because it acts for a controller in the UK. If the link between its handling of data and the controller's UK activities is weak, it's unlikely to be covered. The processor will still be bound by contract to comply with data protection standards – but in such cases, we’d take action against the controller rather than the processor.

Crown dependencies

Does UK data protection law apply in the Isle of Man or the Channel Islands?

No - UK data protection law only applies in England, Northern Ireland, Scotland and Wales.

The Isle of Man and the Channel Islands are not technically part of the UK. They are Crown Dependencies. This means the UK is responsible for their defence and security, but they have their own separate status, government and laws. They have their own data protection law and independent data protection regulators:

- Isle of Man: Isle of Man Information Commissioner (inforights.im)
- Jersey: Jersey Office of the Information Commissioner (jerseyoic.org)
- Guernsey (this also includes Alderney, Sark and a number of smaller islands): Office of the Data Protection Authority (odpa.gg)

They also count as ‘third countries’, so transfers of data need to follow the usual rules for international transfers. But there are UK GDPR adequacy regulations in place, so most UK organisations can send data to these places without needing transfer safeguards.

This is similar to the position for British Overseas Territories – although they have a slightly different historical and constitutional status (and most of them don't have adequacy). See: What are British Overseas Territories and how does DP law apply?

British Overseas Territories

What are British Overseas Territories and how does DP law apply?

UK data protection law doesn't apply in the British Overseas Territories - it only applies in England, Northern Ireland, Scotland and Wales.

The British Overseas Territories are:

- Anguilla
- Bermuda
- British Antarctic Territory (BAT)
- British Indian Ocean Territory (BIOT)
- Cayman Islands
- Falkland Islands
- Gibraltar
- Montserrat
- Pitcairn, Henderson, Ducie and Oeno Islands
- St Helena, Ascension and Tristan de Cunha
- South Georgia and the South Sandwich Islands
- The Sovereign Base Areas of Akrotiri and Dhekelia in Cyprus
- Turks and Caicos Islands
- British Virgin Islands

The UK is responsible for the defence and security of these overseas territories, but they are not part of the UK, and they have their own

independent laws. Not all of the overseas territories have a data protection law – but if they do, they generally have their own independent regulator separate from the ICO. For example, Gibraltar has the Gibraltar GDPR, and the Gibraltar Regulatory Authority (GRA) – see www.gra.gi/data-protection.

The position in the Sovereign Base Areas (military bases) in Cyprus is slightly unusual. The UK and Cyprus agreed that the laws on the bases will mirror Cypriot laws – which means the EU GDPR still applies there. As they are UK territory, the ICO has agreed to act as the local regulator. But that's separate from our role as UK regulator and doesn't change the legal position in terms of which law applies, or whether there's a transfer. If you need to know more about this, email us for specific advice.

Overseas territories count as 'third countries', so transfers of data to the overseas territories need to follow the usual rules for international transfers. Gibraltar has adequacy, but transfers to other territories will need a transfer safeguard in place.

Territorial scope and embassies

Does the UK GDPR apply to foreign embassies in the UK?

Yes, in theory - although in practice we won't be able to enforce.

A foreign embassy or consulate inside the UK is not technically overseas territory. It's in the territory of the UK - so in theory, the UK GDPR does apply to the activities of that establishment in the UK, and we'd generally expect them to comply with local law as a matter of diplomatic convention.

However, consulates and embassies benefit from various legal immunities and privileges under international law (eg the Vienna Convention). In practice, this means that we are very unlikely to be able to take any action to enforce compliance.

The position of UK embassies in other countries is a bit different. The UK GDPR applies in the normal way under Article 3(3) - because even though

those embassies are outside the UK, international law means that UK law still applies. This is explained in recital 25.

EU agencies

Does the UK GDPR apply to EU agencies?

Yes, in theory it can – although it would be unusual and in practice we might find it difficult to enforce.

The UK GDPR doesn't have a specific exemption for EU agencies. So, in theory, it can apply to an EU agency if it's monitoring or offering services to people in the UK.

But if this comes up, it's best to get legal advice.

Note that the EU GDPR doesn't apply to EU institutions and bodies. This is because there's a separate EU data protection regime for them: Regulation (EU) 2018/1725. There's also a specific regulator, the European Data Protection Supervisor (EDPS), which might be best placed to take action.

Remember that any UK organisation that shares personal information with an EU agency will be making a restricted transfer. But transfers to EU bodies can go ahead as they are covered by adequacy regulations.

UN agencies

Does the UK GDPR apply to UN agencies?

Yes, in theory it can – although in practice we wouldn't be able to enforce.

The UK GDPR doesn't have a specific exemption for UN agencies (or other international bodies). So, in theory, it can apply to a UN agency if it's based in the UK, or it monitors or offers services to people in the UK.

However, UN treaties grant UN agencies some legal immunities from local laws. This means that we are unlikely to be able to take any action to enforce compliance. If this comes up, you should ask for legal advice.

This is similar to the situation for embassies – see Does the UK GDPR apply to foreign embassies in the UK?

UN bodies are subject to the UN's own principles on personal data protection and privacy (unsceb.org) – but that's outside our remit.

Remember that any UK organisation that shares personal information with a UN agency (even one based in the UK) will be making a restricted transfer. The usual transfer rules apply, and so the organisation must think about transfer safeguards. See What's a transfer to an international organisation? [2]

2. Establishments

Establishments

What's an establishment?

An individual who's a UK resident is considered to have an establishment in the UK. So is a company, other corporate body, partnership or unincorporated association which is formed under UK law.

But other organisations may still have a UK establishment if they have a presence inside the UK.

Any 'stable arrangement' carrying out 'real and effective activities' (even where it's quite minimal) within a territory can count as an establishment. This isn't easy to define, but the following points can help you identify an establishment. The important point here is that this is about what is actually happening in practice, not about the legal structure on paper.

An establishment doesn't need to take any particular legal form. This means you don't need to look at the legal structure of a company in any detail. In particular, an establishment doesn't have to be a registered office, and it doesn't have to be part of the same legal entity.

So a branch, office, or subsidiary can count as an establishment. So can a single employee or any other agent (i.e. someone acting on behalf of the controller) stationed in a particular country, if this amounts to a 'stable arrangement'. However, an employee temporarily travelling on business wouldn't count as an establishment, because this wouldn't be considered a 'stable arrangement'.

Remember there must also be a link between the use of the data and the activities of the establishment. See Is processing linked to the activities of an establishment?

Establishments and websites

Can a website be an establishment?

A website accessible from the UK isn't automatically a UK establishment.

For example, if an Australian rock band has a website which UK fans regularly use, that's not a UK establishment. However, you might still need to consider whether the website is 'targeting' UK customers.

See also What's an establishment? and What does targeting mean?

Establishments and processors

Can a processor be an establishment of a controller?

You should look at the establishments of controllers and processors separately.

A controller won't have a UK establishment just because it uses a UK processor. A processor isn't an establishment of the controller unless it would be considered an establishment for another reason (e.g. because it is also a subsidiary of the overseas parent controller).

For example, if a US company employs a separate UK processor but has no other presence in the UK, it will not have a UK establishment.

However, if a US company uses its own UK subsidiary as a processor, that will count as a UK establishment. You'll then need to ask whether there is a link between the handling of the data and the activities of the UK subsidiary. See Is processing linked to the activities of an establishment?

Equally, a processor won't have a UK establishment just because it's instructed by a UK controller. See How does territorial scope apply to processors?

See also What's an establishment?

Establishments and activities

Is processing linked to the activities of an establishment?

If you can identify a UK establishment, you still need to ask whether the specific processing activity is **in the context of the activities** of that establishment.

Not everything will be caught. The focus is on each processing activity, not the organisation as a whole. The test is whether the handling of the data is inextricably linked to the activities of the UK establishment (even if someone else actually handles the data for them).

For example, just because a US company has a UK subsidiary (which will count as an establishment), that doesn't mean everything the US company does falls within the scope of the UK regime. Only processing which has a link to the UK subsidiary's business activities will be in scope.

If the processing is linked to the activities of a UK establishment, the UK regime applies. It doesn't matter if the handling of the data itself takes place outside the UK, or the data subjects are outside the UK.

See also What's an establishment?

3. Targeting

Targeting activities

What does targeting mean?

'Targeting' people in the UK means either offering goods or services to people in the UK, or monitoring the behaviour of people in the UK.

The term 'targeting' is not used in the legislation itself, but it can be a useful umbrella term to cover these kinds of activities of overseas organisations which are caught by the UK regime.

Targeting goods and services

What counts as offering goods and services to people in the UK?

In short, there must be evidence that the organisation intends to specifically target customers who are inside the UK.

This is only relevant if an organisation has no UK establishment.

This must be more than just a neutral offer to the world at large. It's not enough that goods or services are in fact provided to UK customers, if this is incidental. For example, a Canadian mail-order company selling goods to a customer in the UK will not automatically be caught.

In particular, it's not enough just to show that a website is accessible in the UK. There must be other evidence of intentional targeting of UK customers – for example:

- a UK marketing campaign;
- a UK custom listing for an app in the app store;
- a website with a ".co.uk" domain name;
- paying search engines to direct traffic from the UK to the website;

- listing prices in pound sterling (GBP);
- UK customer testimonials;
- specific delivery arrangements for UK customers; or
- specific contact details for UK customers.

One of these may well be enough evidence - but it's not automatic. You need to be confident that it clearly shows (when taken with everything else) that they intend to target UK customers.

The individuals must be physically in the UK at the time the relevant use of data takes place. So a business located outside the UK providing services to tourists travelling in that country will not be caught just because those tourists are UK citizens.

If the services are targeted at people who are in the UK, it doesn't matter if those individuals are UK citizens, UK residents or just visitors to the UK. Everyone in the UK benefits from the protection of the UK GDPR. It is the physical location of the individual that matters, not where they are from.

Targeting: monitoring behaviour

What counts as monitoring the behaviour of people in the UK?

This is only relevant if there is no UK establishment.

As a general rule, monitoring behaviour means collecting data about an individual's actions, with the intent to analyse that data and reuse it to profile an individual or make decisions about them.

The tribunal has said it's more than just identification - it must include establishing other facts about a person (eg where they are, who they're with or what they're doing). But it doesn't have to be repeated over time: an organisation can monitor someone at a single point in time. See the Clearview case summary[1].

It doesn't have to be the organisation itself that does the monitoring - it's enough if its handling of data is related to another organisation's monitoring. Again, see the Clearview case summary[1].

The individual must be physically in the UK when they are being monitored. If they are in the UK, it doesn't matter if those individuals are UK citizens, UK residents or just visitors to the UK. Everyone in the UK benefits from the protection of the UK GDPR. It's the physical location of the individual that matters, not where they are from.

Recital 24 of the UK GDPR specifically refers to tracking internet users in order to take decisions, or analyse or predict preferences, behaviours and attitudes. However, this doesn't mean we only look at online tracking - other types of monitoring may still be caught. And it won't include all data collected online, unless the organisation intends to use this data for some kind of behavioural analysis or profiling.

For example, monitoring is likely to cover things like:

- tracking online activity for behavioural advertising purposes;
- tracking user activity to personalise a service;
- using cookies for other tracking purposes;
- tracking device location data;
- wearable devices for monitoring fitness and health; and
- video monitoring.

It's not likely to cover a website just because it's using cookies to record consent preferences or deliver a service, unless that data is reused for profiling or marketing purposes, or for personalisation of the service.

IP address and physical location

Does an IP address show where someone's physically located?

Not always – an IP address only indicates the location of someone's internet connection, not their physical location.

And if someone's using a virtual private network (VPN), they could be hiding their IP address and actual physical location.

So, we don't think organisations can rely on IP addresses to confirm where someone's physically located – which might be relevant, for example, when identifying international transfers. Organisations should have other methods to identify where a recipient of personal information is physically located.
See What counts as a restricted transfer?

4. Representatives

UK Representatives

When do organisations need a UK Representative?

Organisations who don't have a UK establishment but who target people in the UK (by offering goods or services to people in the UK, or monitoring the behaviour of people in the UK), generally need to appoint someone to act as their representative in the UK.

This includes organisations in the EEA.

There is an exemption for public authorities, and for occasional low-risk processing.

The representative acts as a point of contact for individuals and the ICO, but they don't undertake any other business activity related to the processing. They act as an agent of the organisation they represent, not a separate controller or processor.

UK representatives and occasional processing

What does 'occasional processing' mean?

The obligation for overseas organisations to appoint a representative in the UK doesn't apply for occasional processing which is low-risk.

There's no legal definition of what "occasional" processing is. But EDPB guidance suggests this means "if it is not carried out regularly, and occurs outside the regular course of business or activity of the controller or processor".

In general, it's going to depend on the specific circumstances for each organisation, and the processing they are doing in connection with targeting people in the UK.

We'd suggest that organisations take a cautious approach to whether they consider this processing is occasional or not, and they are very sure this processing isn't part of their normal activities, and won't impact on the individuals concerned.

Action against representatives

Can we take action against representatives?

No, not directly. Organisations outside the UK may need to appoint a representative in the UK, but that representative is just a point of contact.

The existence of a representative makes it easier to take action against the controller (or processor). However, any enforcement action is still directed to the controller (or processor) itself, rather than to the representative.

A representative isn't the same as an establishment. They act as a point of contact for individuals and regulators, but they don't undertake any other business activity related to the processing.

Controllership and representatives

Are UK representatives controllers or processors?

Neither - UK representatives appointed by non-UK organisations are 'agents' of the organisation they work for. They aren't separate controllers or processors in their own right when acting in their capacity as a representative .

However, a representative is a separate controller for any personal data they process to run their own business (eg for their own employee data). And if a representative were to start processing personal data outside the scope of their role as a representative (ie for their own distinct purpose), they will become a separate controller in their own right for that processing.

Transfers and UK representatives

Is it a restricted transfer to send data between an organisation and its UK representative?

No. If an organisation has appointed a representative in the UK, that representative is an agent of the organisation itself. The representative is not a processor (or a separate controller) when acting in its capacity as a representative.

This means when a UK representative sends data on to the overseas organisation as part of its role as a UK point of contact, it's essentially the organisation sending data to itself. There is no need to have SCCs or other transfer tools in place.

Of course, the representative will still be a separate controller for data it handles for its own business purposes, outside its role as a contact point. For example, for its own employee data.

EU Representatives

When do UK controllers need an EU representative?

UK organisations who don't have an establishment in the EEA but offer goods or services to people in EEA, or monitor the behaviour of people in the EEA, generally need to appoint someone to act as their representative in the EEA.

There is an exemption for public authorities, and for occasional low-risk uses of data.

The representative acts as a point of contact for individuals and EU regulators, but doesn't undertake any other business activity related to the use of the data, and isn't directly liable for the data protection failings of those it represents.

For more information, see our guidance on European representatives.

5. Enforcement

Action against non-UK organisations

Can we take action against organisations outside the UK?

We can only take action if the processing falls within the territorial scope of the UK regime.

This generally means we can only take action against organisations outside the UK if they either have some kind of stable presence (an 'establishment') inside the UK, or are 'targeting' individuals in the UK.

We can't take action just because affected individuals are UK citizens or live in the UK unless the case falls into one of the categories above.

See What's the territorial scope of the UK GDPR?

Action against representatives

Can we take action against representatives?

No, not directly. Organisations outside the UK may need to appoint a representative in the UK, but that representative is just a point of contact.

The existence of a representative makes it easier to take action against the controller (or processor). However, any enforcement action is still directed to the controller (or processor) itself, rather than to the representative.

A representative isn't the same as an establishment. They act as a point of contact for individuals and regulators, but they don't undertake any other business activity related to the processing.

See also:

When do organisations need a UK representative?
Are UK representatives controllers or processors?

Breach reporting and cross border processing

Who should an organisation report breaches to if they operate in both the UK and the EEA?

Organisations that operate in both the UK and in Europe may need to submit details of any reportable breaches to both the ICO and EU authorities.

For more on when they need to report breaches to us, see: When should a breach be reported under the UK GDPR? [3]

They may also need to report breaches to the data protection authorities in any European countries where people may have been affected, under EU law. But this is outside our remit so they should contact the relevant European authorities for advice or guidance.

6. Territorial scope of EU law

Territorial scope of the EU GDPR

What's the territorial scope of the EU GDPR?

The EU GDPR applies to any organisation (including UK organisations):

- with an **establishment** inside the EEA – the EU GDPR will apply to processing linked to the activities of that establishment; or

- which is outside the EEA but **targets individuals** inside the EEA by offering them goods or services, or monitoring their behaviour – the EU GDPR will apply to processing related to that targeting activity. Organisations in this category usually need to appoint a representative in the EU.

This means some UK organisations will need to comply with both the UK GDPR and the EU GDPR. They may need to deal with both the ICO and other data protection authorities in the EEA.

From 1 January 2021, the ICO no longer regulates the EU GDPR and we can't provide advice on it. UK organisations may need to contact EU data protection authorities for more information and advice.

See also What's the territorial scope of the UK GDPR?

EU Representatives

When do UK controllers need an EU representative?

UK organisations who don't have an establishment in the EEA but offer goods or services to people in EEA, or monitor the behaviour of people in the EEA, generally need to appoint someone to act as their representative in the EEA.

There is an exemption for public authorities, and for occasional low-risk uses of data.

The representative acts as a point of contact for individuals and EU regulators, but doesn't undertake any other business activity related to the use of the data, and isn't directly liable for the data protection failings of those it represents.

For more information, see our guidance on European representatives.

EDPB territorial guidelines

What do we think about EDPB guidelines on territorial scope?

The European Data Protection Board (EDPB) has published guidelines on the territorial scope of the EU GDPR.

The ICO was involved in EDPB discussions on these guidelines and we think they are a useful reference on territorial scope. Scroll down for a quick summary of the guidelines. We take a similar approach to the territorial scope of the UK GDPR.

Remember, EDPB guidelines don't apply in the UK. They can still provide helpful insight on some issues, but we'd always recommend you check ICO guidance first. See: What's the status of EDPB guidance? [4]

Breach reporting and cross border processing

Who should an organisation report breaches to if they operate in both the UK and the EEA?

Organisations that operate in both the UK and in Europe may need to submit details of any reportable breaches to both the ICO and EU authorities.

For more on when they need to report breaches to us, see: When should a breach be reported under the UK GDPR?[3]

They may also need to report breaches to the data protection authorities in any European countries where people may have been affected, under EU law. But this is outside our remit so they should contact the relevant European authorities for advice or guidance.

EU agencies

Does the UK GDPR apply to EU agencies?

Yes, in theory it can – although it would be unusual and in practice we might find it difficult to enforce.

The UK GDPR doesn't have a specific exemption for EU agencies. So, in theory, it can apply to an EU agency if it's monitoring or offering services to people in the UK.

But if this comes up, it's best to get legal advice.

Note that the EU GDPR doesn't apply to EU institutions and bodies. This is because there's a separate EU data protection regime for them: Regulation (EU) 2018/1725. There's also a specific regulator, the European Data Protection Supervisor (EDPS), which might be best placed to take action.

Remember that any UK organisation that shares personal information with an EU agency will be making a restricted transfer. But transfers to EU bodies can go ahead as they are covered by adequacy regulations.

[1] Clearview AI Inc. v The Information Commissioner [2023]

Daniel Hovington
Lawyer

Case Citation

Clearview AI Inc v The Information Commissioner [2023] UKFTT 00819 (GRC)

Case Type

Judgment of the First Tier Tribunal (General Regulatory Chamber) (Information Rights)

Status

Judgment Handed Down

Background and summary of the case before the Tribunal

Clearview is a US company with no presence in the UK or EU. It offers a service to overseas governments and law enforcement agencies, using facial recognition to match images of suspects with images in its database, which have been scraped from the internet (eg from social media). It doesn't currently offer this service to UK agencies, or to any commercial clients.

The ICO took part in a joint investigation with the Australian regulator, focusing on the use of people's images, scraping data from the internet and the use of facial recognition. We issued an enforcement notice and monetary penalty in May 2022, fining Clearview £7.5m.

Clearview appealed, arguing that the ICO had no jurisdiction because they weren't established in the UK, offering services in the UK or monitoring the behaviour of people in the UK - and also that the UK GDPR didn't apply to

their clients' activities, as UK law doesn't apply to overseas government agencies.

We argued that Clearview was itself monitoring the behaviour of people in the UK, by collecting and indexing images of them, and that its use of data was also related to its clients' monitoring activities.

Summary of the Decision

The tribunal decided:

- **What counts as monitoring:** monitoring of behaviour means more than just identification - it must include establishing other facts about a person (eg where they are, who they're with or what they're doing). But it doesn't have to be repeated over time - an organisation can monitor someone at a single point in time.
- **Whose monitoring activities:** as a matter of law, the UK GDPR can apply to one organisation if its use of data is related to monitoring activities undertaken by a different organisation. Here, applying Article 3, Clearview's own collection, indexing and storing of images was related to the clients' monitoring of people's behaviour (even though Clearview itself was not monitoring).
- **Overseas government agencies:** however, applying Article 2, the UK GDPR does not apply to the activities of overseas governments or law enforcement agencies. So the UK GDPR does not apply while Clearview's client base is limited to these agencies.

This meant the ICO did not have the jurisdiction to take any action.

[2] What's a transfer to an international organisation?

This covers sending data to bodies like UN or EU agencies.

‘International organisation’ is defined in Article 4 of the UK GDPR. It means a body governed by public international law, or set up under an international treaty. This covers things like UN agencies - even if they are based in the UK (eg the International Maritime Organisation). It doesn't have anything to do with multinational companies.

The usual transfer rules apply, and organisations sending data to these bodies need to think about transfer safeguards.

It is possible for an international organisation to have adequacy. There is currently a UK adequacy decision in place to cover transfers to EU or EEA institutions, bodies, offices or agencies. But there's no adequacy decision at the moment for the UN or its agencies.

In some cases, a transfer derogation (exception) might apply. In particular, if the UK has signed a treaty which provides for international co-operation for specified reasons, and recognised this in UK law, the derogation in Article 49(1)(d) for 'important reasons of public interest' could be relevant.

[3] **When should a breach be reported under the UK GDPR?**

A ‘personal data breach’ means a breach of security leading to the “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

If the breach causes a likely risk to individuals’ rights and freedoms, they must report it to us within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk to the individuals’ rights and freedoms, they must be informed without undue delay. We can compel controllers to do this if they refuse.

[4] **EDPB guidance**

What's the status of EDPB guidance?

EDPB guidelines are no longer directly relevant to the UK regime.

However, they may still provide helpful guidance on certain issues, and so organisations may want to consult them, and take them into account. In many cases, if an organisation previously relied on the approach set out in EDPB guidance, then they don't need to change that, and it's likely to be an indicator of good practice.

Of course, there may be some areas where the UK and EU regimes may differ slightly (eg international transfer mechanisms), and ICO guidance will be more tailored for UK organisations. We'd always suggest organisations and individuals checked the guidance on our website.