

## What to do if Union law has been breached?

If you are a national of a country of the European Union, or if you live in one of these countries, or if you run a business in the European Union, Union law gives you a number of rights.

If you would like to know more, you can:

- [Ask a question about the EU \(Europe Direct\)](#)
- [Find out more about your EU rights when moving around in the EU \(Your Europe\)](#)
- [Ask a question about your rights in a situation you are facing in the EU \(Your Europe Advice\)](#).
- [Find out more about the national justice systems throughout the EU \(e-Justice\)](#).

If you feel that your rights under Union law have not been respected by the national authorities of a country of the European Union, you should first of all take up the matter with national bodies or authorities. This will often be the quickest and most effective way to resolve the issue.

### Available means of redress at national level

As stated in the Treaties, public authorities and national courts have the main responsibility for the application of Union law.

Therefore, it is in your interest to make use of all possible means of redress at national level (administrative and/or out-of-court mediation mechanisms).

Depending on the system of each country, you may also submit your file to the [national ombudsmen](#) or [regional ombudsmen](#).

Or you can bring your matter to the court of the country where the problem occurred. [Find out more about national judicial systems or going to court](#). If solving your problem requires the annulment of a national decision, be aware that only national courts can annul it. If you are seeking compensation for damage, only national courts have the power, where appropriate, to order national authorities to compensate individuals for losses they have suffered due to a breach of Union law.

### Other problem-solving instruments

Alternatively, you may wish to:

- **contact SOLVIT**- SOLVIT is a service provided by the national administration, which deals with cross-border problems related to the misapplication of Union law by national public administrations in the Internal Market. There is a SOLVIT centre in every EU country, as well as in Norway, Iceland and Liechtenstein. Your Country will try to solve the problem with the other Country concerned. Going through SOLVIT might take less time than making a formal complaint to the European Commission and can solve your individual problem. If a problem goes unresolved, or you consider that the proposed solution is unacceptable, you can still pursue legal action through a national court or lodge a formal complaint with the European Commission. Please be aware that addressing the issue to SOLVIT does not suspend time limits before national courts.

[Submit your problem to SOLVIT](#)

- **contact European Consumer Centres** - there is a Europe-wide network of consumer centres, which cooperate to help settle disputes between consumers and traders based in different EU countries, as well as in Norway, Iceland and Liechtenstein.

[Submit your problem to European Consumer Centres](#)

- **contact FIN-Net** - which is a network for resolving financial disputes out of court in EU countries, as well as in Iceland, Liechtenstein and Norway. They are responsible for handling disputes between consumers and financial services providers.

[Submit your problem to FIN-Net](#)

## Available actions at EU Level

Although you will usually be able to enforce your rights better in the country where you live, the European Union may also be able to help you:

- **The Committee on Petitions of the European Parliament**

You have the right ([Article 227 TFEU](#)) to submit a petition to the European Parliament about the application of Union law. You may submit your petition by post or online via the [European Parliament's website](#). You can find out more about petitions to the European Parliament on the [EU citizenship and free movement website](#).

- **The European Commission**

You can contact the European Commission about any measure (law, regulation or administrative action), absence of measure or practice by a country of the European Union that you think is against Union law.

The European Commission can only take up your complaint if it is about a breach of Union law by authorities in an EU country. If your complaint is about the action of a private individual or body (unless you can show that national authorities are somehow involved), you have to try to solve it at national level (courts or other ways of settling disputes). The European Commission cannot follow up matters that only involve private individuals or bodies, and that do not involve public authorities.

If you are not an expert in Union law, you may find it difficult to find out exactly which Union law you think has been breached. You can get advice quickly and informally from the Your Europe Advice service, in your own language.

- **The European Ombudsman**

If you consider that the European Commission has not dealt with your request properly, you may contact the [European Ombudsman](#) ([Articles 24 and 228 TFEU](#)).

## How to submit a complaint to the European Commission

You must submit your complaint via the standard complaint form, which you can fill out in any [official EU language](#). Please make sure you include the following details:

- Describe exactly how you believe that national authorities have infringed Union law, and which is the Union law that you believe they have infringed.
- Give details of any steps you have already taken to obtain redress.

## What does the European Commission do with your complaint?

- The European Commission will confirm to you that it has received your complaint within 15 working days.
- The European Commission will invite you to resubmit your complaint in case you have not used the standard complaint form.
- Within the following 12 months, the European Commission will assess your complaint and aim to decide whether to initiate a formal infringement procedure against the country in question. If the issue that you raise is especially complicated, or if the European Commission needs to ask you or others for more information or details, it may take longer than 12 months to reach a decision. You will be informed if the assessment takes longer than 12 months. If the European Commission decides that your complaint is founded and initiates a formal infringement procedure against the country in question, it will inform you and let you know how the case progresses.
- Should the Commission contact the authorities of the country against which you have made your complaint, it will not disclose your identity unless you have given your express permission

to do so.

- If the European Commission thinks that your problem could be solved more effectively by any of the available informal or out-of-court problem-solving services, it may propose to you that your file be transferred to those services.
- If the Commission decides your problem does not involve a breach of Union law, it will inform you by letter before it closes your file.
- At any time, you may give the European Commission additional material about your complaint or ask to meet representatives of the European Commission.

Find out more about how the European Commission handles its relations with complainants: [Communication on the handling of relations with the complainant in respect of the application of Union law.](#)

There are two ways of submitting a complaint:

- **via internet:** SG-PLAINTES@ec.europa.eu
- **by post:**

European Commission Secretary-General  
B-1049 Brussels BELGIUM

Or

[EU Commission office in your country](#)

Or

by fax: 3222964335

### **What the Commission can and cannot do**

After examining the facts of your complaint, the Commission will decide whether further action should be taken. The Commission may decide not to open a formal infringement procedure, even if it considers that a breach of EU law has occurred. For instance, the Commission may consider that a national or EU level redress mechanism is in a better position to deal with your complaint.

In 2017, the Commission closed complaints received [in the area of gambling](#). The Commission did not consider it a priority to use its enforcement powers to promote an EU Single Market in the area of online gambling services. Complaints in the gambling sector can be handled more efficiently by national courts than by the Commission.

On the other hand, if the Commission takes a country to the Court of Justice and wins the case, the country will have to take all actions to remedy the violations.

If the Commission brings the case before the Court of Justice of the European Union, it may take several years for the Court of Justice to hand down its judgment. Judgments of the Court of Justice differ from those of national courts. The Court of Justice delivers a judgment stating whether there has been an infringement of European Union law. The Court of Justice cannot annul a national provision which is incompatible with European Union law, nor force a national administration to respond to the request of an individual, nor order the country to pay damages to an individual adversely affected by an infringement of European Union law. To seek compensation, complainants must still take their case to a national court within the time limit set out in national law.

### **Multiple complaints**

Where a number of complaints are lodged in relation to the same grievance, the Commission may register them under the same number.

Individual acknowledgements and letters may be replaced by a notice on the Europa website.

[Multiple complaints receipt confirmations](#)

[Decisions taken on multiple complaints](#)



Before filling in this form, please read 'How to submit a complaint to the European Commission':

[https://ec.europa.eu/assets/sg/report-a-breach/complaints\\_en/](https://ec.europa.eu/assets/sg/report-a-breach/complaints_en/)

All fields with \* are mandatory. Please be concise and if necessary continue on a separate page.

## 1. Identity & contact details

	Complainant*	Your representative (if applicable)
Title* Mr/Ms/Mrs	Mr	
First name*	Tomaso	
Surname*	Falchetta	
Organisation:	Privacy International	
Address*	62 Britton Street	
Town/City *	London	
Postcode*	EC1M 5UY	
Country*	U.K.	
Telephone		
E-mail	tomasof@privacyinternational.org	
Language*	English	
Should we send correspondence to you or your representative*:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

	Complainant*	Your representative (if applicable)
Title* Mr/Ms/Mrs	Ms	
First name*	Megan	
Surname*	Goulding	
Organisation:	Liberty	
Address*	Liberty House, 26-30 Strutton Ground	
Town/City *	London	
Postcode*	SW1P 2HR	
Country*	U.K.	
Telephone		
E-mail	MeganG@libertyhumanrights.org.uk	
Language*	English	
Should we send correspondence to you or your representative*:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

	Complainant*	Your representative (if applicable)
Title* Mr/Ms/Mrs	Mr	
First name*	Jim	
Surname*	Killock	
Organisation:	Open Rights Organisation	

Address*	Unit 7, Tileyard Acorn Studios, 103-105, Blundell Street	
Town/City *	London	
Postcode*	N7 9BN	
Country*	U.K.	
Telephone		
E-mail		
Language*	English	
Should we send correspondence to you or your representative*:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## 2. How has EU law been infringed?\*

	Authority or body you are complaining about:
Name*	UK Government (Home Office)
Address	
Town/City	
Postcode	
EU Country*	U.K.
Telephone	
Mobile	
E-mail	

### 2.1 Which national measure(s) do you think are in breach of EU law and why?\*

<p>UK's legal framework for the retention and access of communications data is in breach of EU law.</p> <p>In particular:</p> <ul style="list-style-type: none"> <li>- Part 4 of the Investigatory Powers Act 2016 [retention of communications data]</li> <li>- Part 3 of the Investigatory Powers Act 2016 [access to communications data]</li> </ul> <p>These provisions do not comply with EU law in so far as:</p> <ul style="list-style-type: none"> <li>- they allow mass retention of communications data;</li> <li>- they allow a wide range of authorities access to such data for a wide, ill-defined range of purposes and without adequate safeguards.</li> </ul>
--

### 2.2 Which is the EU law in question?

<ul style="list-style-type: none"> <li>- Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union (the “<b>Charter</b>”);</li> <li>- Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (the “<b>e-Privacy Directive</b>”).</li> <li>- As interpreted by the Court of Justice of the European Union in <i>Tele2/Watson</i> and <i>Digital Rights Ireland</i>, where the Court held that the ePrivacy Directive when read in light of the Charter, prohibits</li> </ul>
---

national legislation from imposing data retention obligations unless it is “strictly necessary” for the purpose of fighting “serious crime” and that measures allowing for “general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication” are not permitted. The CJEU held that law enforcement agencies can only access the retained data where it is “strictly necessary” for the purpose of fighting serious crime and where such access has been approved following a prior review by a court or independent authority.

### 2.3 Describe the problem, providing facts and reasons for your complaint\* (max. 7000 characters):

The complainants raise concerns about the retention and access regimes of communications data in the UK.

The issues relate to the Investigatory Powers Act 2016 (the “Act”).

#### **Retention** (*Part 4 of the Act*)

Part 4 regulates retention of communications data. Under s.87 the Secretary of State can require any telecommunication operator to retain all or any description of communications data (and entity data) for up to 12 months.

In a context where the gathering and exploitation of data by private companies becomes increasingly intrusive and widespread, data retention poses serious risks to individual privacy and data security. The data opens the door for governments and third parties to access it in order to make intimate inferences about individuals, to engage in profiling and to otherwise intrude on people’s private lives. If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including cybercriminals.

#### *EU law*

Privacy is afforded protection under the Charter at Article 7 (respect for private and family life) and Article 8 (protection of personal data) as well as under the limitations and guarantees of Article 52.

The ePrivacy Directive, Article 15, provides that “Member States may...adopt legislative measures providing for the retention of data for a limited period [where data retention constitutes] a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system [and provided the data retention measures are] in accordance with the general principles of Community law”.

Another Directive, No. 2006/24, was adopted to ensure harmonisation between Member States’ retention regimes and to impose an obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data generated or processed by them. In its judgment in *Digital Rights Ireland* of April 2014, the CJEU held Directive 2006/24 to be invalid as a disproportionate exercise of the EU legislature’s powers in breach of Articles 7, 8 and 52(1) of the Charter.

In December 2016, the CJEU in *Tele2/Watson* reaffirmed *Digital Rights Ireland* and expanded on it. The judgment positively asserted minimum safeguards of EU law that must be prescribed in any national data retention/access legislation – in this regard, the CJEU held:

- a general and indiscriminate data retention obligation could never be compatible with EU law; in particular, Article 15 of the ePrivacy Directive, read in the light of the Charter, “must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication” (¶1 dispositif);

- retention of data is permitted if it is targeted, for the purpose of fighting serious crime, and retention is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary (¶¶102, 108);
- substantive conditions that must be satisfied to authorise data retention may vary, but retention must meet objective criteria that establish a connection between the data to be retained and the objective pursued (¶110);
- national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least indirect, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security (¶111);
- national legislation must require a reasoned application from a national authority to request interception or access, and access (unless urgent) should be subject to a prior review by a court or independent body (¶120);
- national legislation must require notification of any person affected as soon as that notification is no longer liable to jeopardise the investigations undertaken (¶121);
- national legislation must require that data be retained within the EU and be irreversibly destroyed at the end of the retention period, and that providers of electronic communications services guarantee a particularly high level of protection (¶122); and
- national legislation must ensure review, by an independent authority, of compliance with the level of data protection required by EU law (¶123).

#### *Application of EU law in UK context and continuing incompatibility*

In applying the findings of *Tele2/Watson* to the relevant UK legislation at the time – the Data Retention and Investigatory Powers Act 2014 (“**DRIPA**”) – the UK Court of Appeal declared in January 2018 that it was incompatible with EU law in relation to access to retained data, but did not make a declaration applying the conclusion in *Tele2/Watson* on general and indiscriminate data to DRIPA.

It is the complainants’ contention that Part 4 of the Act is incompatible with EU law in that it does provide for the general and indiscriminate retention of data. This is so because the data retained is not limited by reference to categories of data, means of communication or persons concerned and/or Part 4 does not proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious criminal offences – as required by *Tele2/Watson*. Indeed, certain of those features were features that the CJEU picked out in *Digital Rights Ireland* as features of Directive 2006/24 that meant it failed to meet EU human rights standards; if Directive 2006/24 was struck down on those grounds, Part 4 must also be seen as incompatible with EU law for the same reasons – and the fact *Tele2/Watson* laid them out as specific minimum safeguards reinforces that.

Even if Part 4 does not permit general and indiscriminate retention, it is still incompatible with EU law because it still fails to meet the *Tele2/Watson* safeguards (whether or not that amounts to it permitting general and indiscriminate retention).

#### **Access to retained data** (*Part 3 of the Act*)

Part 3 of the Act re-enacts DRIPA in relation to access to such data. Part 3 grants many public authorities the power to self-authorise access to communications data for a list of ten broadly defined purposes where it is necessary and proportionate for them to do so (s.61(7)). Judicial authorisation is required only for local authority access to communications data and requests by authorities for data in order to identify a journalist’s source. In all other cases, a senior officer within an authority will

grant an authorisation and, in exceptional circumstances, this person does not even need to be independent from the investigation.

*Application of EU law in UK context and continuing incompatibility*

The Court of Appeal in *Watson* declared that DRIPA was incompatible with EU law in relation to access to retained data. The Court confirmed two inconsistencies of DRIPA with EU law, in the area of criminal justice: (i) access to retained data is not limited to the purpose of combating “serious crime”; and (ii) access to retained data is not subject to prior review by a court or independent administrative body – requirements that were laid down in *Tele2/Watson*.

These two features of DRIPA that were held to be incompatible with EU law remain in Parts 3 and 4 of the Act, thus making Parts 3 and 4 in relation to access to retained data incompatible with EU law. In July 2017, the Government admitted the Act was “inconsistent with the requirements of EU law”. Despite that admission, however, the Government did not repeal or amend the access provisions of Parts 3 and 4 of the Act; unlawful retention and access to communications data continues.

It is hoped that the Government will amend the legislation to fully comply with EU law on access to retained data. It remains to be seen whether that will happen, and in any event, such amendments will not address all of the issues detailed above.

2.4 Does the Country concerned receive (or could it receive in future) EU funding relating to the subject of your complaint?

Yes, please specify below       No       I don't know

2.5 Does your complaint relate to a breach of the EU Charter of Fundamental Rights?

The Commission can only investigate such cases if the breach is due to national implementation of EU law.

Yes, please specify below       No       I don't know

The legal framework is in breach of Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, and is a national implementation of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

### 3. Previous action taken to solve the problem\*

Have you already taken any action in the Country in question to solve the problem?\*

**IF YES**, was it:  Administrative  Legal ?

**3.1** Please describe: (a) the body/authority/court that was involved and the type of decision that resulted; (b) any other action you are aware of.

#### **Judicial review of DRIPA**

Watson and others lodged, before the UK High Court, applications for judicial review of the legality of s.1 of DRIPA, claiming, inter alia, that that section is incompatible with Articles 7 and 8 of the Charter.

By judgment of 17 July 2015, the High Court held that s.1 of DRIPA is not compatible with Articles 7 and 8 of the Charter in so far as it does not lay down clear and precise rules providing for access to and use of retained data and in so far as access to that data is not made dependent on prior review by a court or an independent administrative body.

The decision was appealed by the Secretary of State for the Home Department. In the judgment of 20 November 2015, the Court of Appeal stayed the proceedings to refer questions for preliminary ruling to the CJEU. The CJEU ruled on these in the *Tele2/Watson* judgment mentioned in detail above.

The Court of Appeal then resumed its consideration of the *Watson* case and gave judgment on 30 January 2018, granting a declaration that DIPA was incompatible with EU law in two respects related to the regime of access of retained data (see above).

#### **Liberty's judicial review challenge to the Act**

Liberty issued a claim for judicial review of various provisions of the Act, including Parts 3 and 4 on retention and access to communications data, on 28 February 2017. On 14 June 2017, the Court granted Liberty permission to challenge Part 4 of the Act and stayed the rest of the claim. A hearing was held on 27-28 February 2018 in relation to Liberty's Part 4 challenge, and the judgment was handed down on 27 April 2018.

In that judgment, the Court held that Part 4 of the Act is incompatible with fundamental rights in EU law in so far retention orders issued for crime-fighting purposes are not limited to the purpose of combating "serious crime", and retention orders are not subject to prior review by a court or an independent administrative body. The Court ordered the Government to amend the Act by 1 November 2018. The Act has yet to be amended, and even if amended will still be legally defective, thus continuing to be incompatible with EU law.

In respect of retention of data, the Court rejected Liberty's contention that Part 4 of the Act was incompatible with EU law because it provides for the general and indiscriminate retention of communications data. Liberty intends to appeal this finding.

**3.2** Was your complaint settled by the body/authority/court or is it still pending? If pending, when can a decision be expected?\*

**Liberty's judicial review challenge to the Act**

**IF NOT** please specify below as appropriate

- Another case on the same issue is pending before a national or EU Court
- No remedy is available for the problem
- A remedy exists, but is too costly
- Time limit for action has expired

4. If you have already contacted any of the EU institutions dealing with problems of this type, please give the reference for your file/correspondence:

- Petition to the European Parliament – Ref:.....
- European Commission – Ref:.....
- European Ombudsman – Ref:.....
- Other – name the institution or body you contacted and the reference for your complaint (e.g. SOLVIT, FIN-Net, European Consumer Centres)

5. List any supporting documents/evidence which you could – if requested – send to the Commission.

 Don't enclose any documents at this stage.

#### 6. Personal data\*

Do you authorise the Commission to disclose your identity in its contacts with the authorities you are lodging a complaint against?

- Yes       No

 *In some cases, disclosing your identity may make it easier for us to deal with your complaint.*