

National DPIA "blacklists"

January 2020



Belgium | China | France | Germany | Italy | Luxembourg | Netherlands | Spain | UK | US - Silicon Valley

Fieldfisher is the trading name of Fieldfisher LLP, a limited liability partnership registered in England and Wales (registered number OC318472) and is authorised and regulated by the Solicitors Regulation Authority. A list of its members and their professional qualifications is available at its registered office, Riverbank House, 2 Swan Lane, London EC4R 3TT. We use the term partner to refer to a member of the Fieldfisher LLP, or an employee or consultant with equivalent standing and qualifications.

Data Protection Impact Assessments

A Data Protection Impact Assessment ("DPIA") is a formal process to help a controller of personal data identify and minimise the data protection risks of a processing activity.

Where the processing of personal data is likely to result in a "high risk" to individuals, Article 35(1) of the General Data Protection Regulation ("GDPR") requires that the controller complete a DPIA before commencing the processing activity.

According to the GDPR, the following scenarios require a DPIA automatically:

- systematic and extensive evaluation of personal aspects of individuals, including profiling, that have a legal effect or similarly significant effect,
- processing of special categories of personal data or criminal record data on a large scale, and
- systematic public monitoring on a large scale.

A DPIA may also be required in other scenarios depending on the nature of the processing activity and the risks involved.

EDPB guidelines and national "blacklists"

The European Data Protection Board ("EDPB") has published guidelines setting out nine criteria that should be considered when determining whether processing involves a "high risk" (the "EDPB criteria").¹ The EDPB criteria include, for example, the use of new technologies, processing on a large scale, evaluation or scoring, matching or combining data sets, and processing that prevents individuals from exercising their rights or obtaining access to a service. In most cases, a DPIA will be required where two or more of the EDPB criteria are met but in some cases a DPIA will be required where only one criterion applies.

In addition, Article 35(4) of the GDPR requires that the supervisory authorities of each EU Member State publish their own lists of scenarios where a DPIA will be required for processing that they supervise – the so-called DPIA "blacklists". The table below provides a high-level overview of the most common scenarios identified by these national "blacklists".

How to read the table

This table is only intended to provide a rough guide to the national "blacklists" and further analysis will be required to determine whether a specific processing activity triggers the need for a DPIA under the GDPR and/or Member State law.

When reading the table, please note the following:

- the table only covers the most common scenarios that appear in the "blacklists" and not all of the scenarios that are identified,
- where a scenario is marked by a tick, a DPIA will be required if that scenario applies or forms a crucial component of the processing activity,
- where a scenario is marked by a cross, a DPIA will only be required if that scenario applies and at least one of the other EDPB criteria also applies, and
- we have given the scenarios broad descriptions and there are inevitably differences as to how each scenario is described and interpreted by each Member State.

Finally, please note our table only includes the Member States that have published "blacklists" at the time of publication of this note².






¹ See WP248 rev.01, Section III(B)(a) (pages 9-11).

² Portugal and Iceland have also published blacklists but English translations were not available at the time of publication of this note and are not therefore included in the table.

Summary of DPIA "blacklists"

Key









- ✓ = DPIA required if this scenario applies or forms a crucial component of the processing activity
- X = DPIA required if this scenario applies and another of the EDPB criteria also applies

Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Invisible" processing ³	Children and vulnerable subjects	Biometric and genetic data	Data of a "highly personal nature" ⁴	Denial of service ⁵
 Austria		✓	✓	✓	X	✓		✓		X	X		
 Belgium	✓	✓		✓	✓						✓	✓	✓
 Bulgaria		✓			✓				✓	✓	✓		
 Croatia		✓	✓	✓	✓	✓	✓	✓		✓	X		✓
 Cyprus		✓		✓		✓	✓	✓			✓		









³ "Invisible" processing refers to scenarios where the controller does not provide notice to individuals on the basis that doing so would be impossible, involve disproportionate effort or seriously impair the processing objective (pursuant to GDPR Article 14(5)(b)).



⁴ Data of a "highly personal nature" may include special categories of personal data (such as health data) as well as other data that may be considered sensitive (such as financial data).

⁵ Denial of service refers to scenarios where the individual is denied access to a product, service, contract, opportunity or benefit.

Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Invisible" processing ³	Children and vulnerable subjects	Biometric and genetic data	Data of a "highly personal nature" ⁴	Denial of service ⁵
 Czech Republic	X	X					X	X		X	X	X	
 Denmark		X	✓	✓	X					X	X		X
 Finland					X				X		X		
 France			✓	✓	✓		✓			✓	✓	✓	✓
 Germany ⁶	✓		✓	✓	✓	✓	✓	✓			X		
 Hungary	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓
 Ireland	✓		✓	✓	✓	✓	✓	✓	✓	✓	X		
 Italy		X	✓	✓	✓	✓	✓	✓		✓	✓	✓	

⁶ This is the blacklist published by the German Data Protection Conference, which applies for the whole of Germany. There are 16 regional supervisory authorities in Germany, some of which have also published their own blacklists.

Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Invisible" processing ³	Children and vulnerable subjects	Biometric and genetic data	Data of a "highly personal nature" ⁴	Denial of service ⁵
 Luxembourg					✓	✓	✓	✓	X		X		
 Netherlands	✓	✓		✓	✓		✓	✓			✓		
 Norway		X		✓	X		✓	✓			X	✓	
 Poland	X	X	X	X	X	X	X	X			X		X
 Romania	✓	✓	✓		✓		✓	✓		✓	✓		
 Slovakia		X		✓		✓	✓	✓	X		X		✓
 Slovenia	✓	✓	✓	✓		✓	✓	✓		✓	✓		✓
 Spain	X	X	X	X	X	X	X	X		X	X	X	X

Country	Large-scale processing	New tech	Automated decision-making	Profiling and evaluation	Location data and tracking	Combining and matching data	Employee monitoring	Public surveillance	"Invisible" processing ³	Children and vulnerable subjects	Biometric and genetic data	Data of a "highly personal nature" ⁴	Denial of service ⁵
 Sweden	X	X	X	X		X	✓	X		X		X	X
 United Kingdom		X		✓	X	✓			X	✓	X		✓