GRC+ SERVICE SHEET · NOVEMBER 2026

Data Protection Impact Assessment (DPIA)

We carry out the DPIA for a new system, supplier or use of data: screening, description, necessity and proportionality, risks to people and the measures that reduce them. You get a signed-off assessment and clear actions before you go live.

SERVICE
Advisory service

USUALLY TAKES
Weeks, usually, from screening to a signed-off DPIA

What It Is

A GDPR Article 35 DPIA for high-risk processing, from screening to a signed-off assessment your DPO and regulator can follow.

Who It Is For

- Screening: is a DPIA required?
- Assessment of risks to the people concerned
- Measures and actions agreed before go-live

What a DPIA Must Cover

Description of the processing	The processing operations and their purposes, including the legitimate interest pursued where that is the legal basis (Art. 35(7)(a)).
Necessity and proportionality	Whether the processing is necessary for its purposes and in proportion to them (Art. 35(7)(b)).
Risks to people	The risks to the rights and freedoms of the people whose data you process (Art. 35(7)(c)).
Measures	The safeguards, security measures and mechanisms that address the risks and show you comply with the GDPR (Art. 35(7)(d)).

How It Runs

1	**Screening** We check whether a DPIA is required and agree the scope.	Week 1
2	**Assessment** Workshops with the business, IT and the supplier.	Week 2
3	**Measures** Risks rated and measures agreed with the owners.	Week 3
4	**Sign-off** The DPIA signed off, with actions tracked to go-live.	Week 4

Regulations That Ask for It

GDPR	A GDPR Article 35 DPIA for high-risk processing, from screening to a signed-off assessment your DPO and regulator can follow.
PDPL (Oman)	
CCPA (United States)	
Data Act	
ePrivacy	
HIPAA (United States)	
EHDS	
NIST Privacy Framework	
FERPA (United States)	
Quebec Law 25 (Canada)	
Alberta PIPA (Canada)	
BC PIPA (Canada)	

Questions Buyers Ask

When is a DPIA required?

Before processing that is likely to result in a high risk to people, for example large-scale sensitive data, systematic monitoring or new technology such as AI. The screening gives you a written answer.

Can our DPO sign off a DPIA you wrote?

Your DPO advises on it rather than signs it. We write the DPIA with the project team, your DPO gives advice (Article 35(2)) and you, as the controller, sign it off.

What is a FRIA?

A fundamental rights impact assessment, required under the AI Act for some deployers of high-risk AI systems. We can combine it with the DPIA.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/data-protection-impact-assessment

