Keepabl
PRIVACY
SECURITY
COMPLIANCE

UK GDPR Reform

The UK Data Protection & Digital Information Bill

3rd version as at 8 November 2023

RoPAs
DPOs & SRIs
DPIAs & Assessments
DSRs

UK GDPR Brexit Reforms

You know the phrase ‘you’re comparing apples and oranges’?

It’s when you’re deliberately (or accidentally) comparing two very different things.

We wanted to put the current obligations in UK GDPR side-by-side with the proposed obligations in the UK Data Protection & Digital Information Bill.

That way we can all compare apples with apples and see what practical changes might happen.

We’d published a similar Guide for DPDI1 back in August 2022. This update is for the third version of the Bill as introduced on 8 November 2023, Bill 001 2023-24.

Accountability

At Keepabl, we focus on the practicalities of Privacy. With that focus, the key changes in the Brexit reforms are to:

- ✓ **RoPAs**
- ✓ **DPOs / SRIs**
- ✓ **DPIAs / Risk Assessments**
- ✓ **DSARs**

The UK government claims that these reforms will: '*[reduce] the burdens on businesses that impede the responsible use of personal data. By giving businesses the opportunity to protect personal data in the most proportionate and appropriate way, we will make them more efficient, meaning higher productivity rates, and more jobs.*'

We've stripped out the rhetoric so you can decide on these claims yourself, apples to apples.

RoPAs

RoPAs - Controllers

UK & EU GDPR

Records of processing activities (Art 30)

1. Each **CONTROLLER** and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

Controllers

(a) name and contact details of the controller, any joint controller, the controller's representative and data protection officer

Purposes

(b) the purposes of the processing

Data Subjects & Personal Data

(c) description of categories of data subjects and categories of personal data

Recipients

(d) the categories of recipients to whom the personal data have been or will be disclosed including in third countries or international organisations

Transfers

(e) transfers to a third country or international organisation, identifying that country or IO and, for Art 49(1), 2nd subpara, documentation of suitable safeguards

Retention

(f) where possible, envisaged time limits for erasure of different categories of data

Security

(g) where possible, a general description of the technical and organisational security measures

UK DPDI Bill

Records of processing of personal data (Art 30A)

2. The **CONTROLLER** must maintain appropriate records of processing of personal data carried out by or on behalf of the controller.
3. The controller's records must include at least the following information about the personal data in respect of which the controller is for the time being a controller:

Purposes

(b) the purposes for which the controller is processing the personal data

Personal Data

(e) whether the personal data includes Art 9(1) special categories of personal data and, if so, which categories

(f) whether the personal data includes Art 10(1) [crime etc] personal data and, if so, which categories

Recipients

(c) the categories of person with whom the controller has shared, or intends to share, the personal data (including persons who are in third countries or IOs)

Location & Transfers

(a) where the personal data is (including information about any personal data that is outside the UK)

Retention

(d) how long the controller intends to retain the personal data

Security

4. where possible, information about how the controller ensures that personal data is secure

Plus UK DPA 2018 Schedule 1 for special categories

RoPAs - Processors

UK & EU GDPR

Records of processing activities (Art 30)

2. Each **PROCESSOR** and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

Controllers

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative and data protection officer

Processing

(b) the categories of processing carried out on behalf of each controller

Transfers

(c) where applicable, transfers to a third country or international organisation, identifying that country or IO and, for Art 49(1), 2nd subpara, documentation of suitable safeguards

Security

(d) where possible, a general description of the technical and organisational security measures

SME Exemption

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in **a risk** to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Art 9(1) or personal data relating to criminal convictions and offences referred to in Art 10.

UK DPDI Bill

Records of processing of personal data (Art 30A)

5. The **PROCESSOR** must maintain appropriate records of its processing of personal data.
6. The processor's records must include at least the following information about the personal data in respect of which it is for the time being a processor:

Controllers

(a) the name and contact details of each controller on behalf of which the processor is acting

Location & Transfers

(b) where the personal data is (including information about any personal data that is outside the UK)

Security

7. where possible, information about how the processor ensures that personal data is secure

Exemption

1. [The Art 30A obligations] apply to a controller [or processor] that carries out processing of personal data which, taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of individuals.

DPOs & SRIs

DPOs & SRIs

UK & EU GDPR

Appointment (Art 37)

Public sector

1. The **controller and the processor** shall designate a DPO in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

Private sector

1. The **controller and the processor** shall designate a DPO in any case where: ...

(b) the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects **on a large scale**; or

(c) the **core activities** of the controller or the processor consist of processing **on a large scale** of special categories of data pursuant to Art 9 and personal data relating to criminal convictions and offences referred to in Art 10

UK DPDI Bill

Appointment (Art 27A)

Public sector

1. Arts 27A, B and C apply to a **controller or processor** that :

(a) is a public body ... other than a court or tribunal acting in its judicial capacity

Private sector

1. Arts 27A, B and C apply to a **controller or processor** that: ...

(b) carries out processing of personal data which, taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of individuals ... other than a court or tribunal acting in its judicial capacity

Qualifiying roles

3. Where the controller or processor is an organisation—

(a) a designated individual must be part of the organisation's senior management

5. In this Article, "senior management", in relation to an organisation, means the individuals who play significant roles in the making of decisions about how the whole or a substantial part of its activities are to be managed or organised.

DPO = Data Protection Officer under GDPR
SRI = Senior Responsible Individual under UK DPDI Bill

DPOs & SRIs - Controllers

UK & EU GDPR

Tasks (Art 39)

1. The DPO shall have at least the following tasks:

Advising

(a) to inform and advise the controller or processor and the employees who carry out processing of their obligations pursuant to GDPR and to other UK / EU or Member State DP provisions ...

(c) to provide advice where requested as regards the DPIA and monitor its performance

Monitoring & Training

(b) to monitor compliance with GDPR, with other UK / EU or Member State DP provisions and with the policies of the controller or processor in relation to the protection of personal data, including assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits

Liaison: Supervisory Authority

(d) to cooperate with the [UK] Commissioner / [EU] supervisory authority

(e) to act as the contact point for the [UK] Commissioner / [EU] supervisory authority on issues relating to processing, including Art 36 prior consultation, and to consult, where appropriate, with regard to any other matter

UK DPDI Bill

Tasks (Art 27B)

1. The SRI designated by a **CONTROLLER** must be responsible at least for performing the tasks listed in paragraph 2 or securing that they are performed by another person.
2. Those tasks are:

Advising

(c) informing and advising the controller, any processor engaged by the controller and employees of the controller who carry out processing of personal data of their obligations under the data protection legislation

Monitoring & Training

(a) monitoring compliance by the controller with the data protection legislation

(d) organising training for employees of the controller who carry out processing of personal data

Liaison: Supervisory Authority

(g) co-operating with the Commissioner on behalf of the controller

(h) acting as the contact point for the Commissioner on issues relating to processing of personal data

Ensuring Compliance

(b) ensuring that the controller develops, implements, reviews and updates measures to ensure its compliance with the data protection legislation

Complaints

(e) dealing with complaints made to the controller in connection with the processing of personal data

Breaches

(f) dealing with personal data breaches

DPOs & SRIs - Processors

UK & EU GDPR

Tasks (Art 39)

1. The DPO shall have at least the following tasks:

Advising

(a) to inform and advise the controller or processor and the employees who carry out processing of their obligations pursuant to GDPR and to other UK / EU or Member State DP provisions ...

(c) to provide advice where requested as regards the DPIA and monitor its performance

Monitoring & Training

(b) to monitor compliance with GDPR, with other UK / EU or Member State DP provisions and with the policies of the controller or processor in relation to the protection of personal data, including assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits

Liaison: Supervisory Authority

(d) to cooperate with the [UK] Commissioner / [EU] supervisory authority

(e) to act as the contact point for the [UK] Commissioner / [EU] supervisory authority on issues relating to processing, including Art 36 prior consultation, and to consult, where appropriate, with regard to any other matter

UK DPDI Bill

Tasks (Art 27B)

3. The SRI designated by a **PROCESSOR** must be responsible at least for performing the tasks listed in paragraph 4 or securing that they are performed by another person.
4. Those tasks are:

Monitoring

(a) monitoring compliance by the processor with Arts 28 [processing agreements], 30A [RoPAs] and 32 [Security]

Liaison: Supervisory Authority

(b) co-operating with the Commissioner on behalf of the processor

(c) acting as the contact point for the Commissioner on issues relating to processing of personal data

DPOs & SRIs

UK & EU GDPR

Conflicts (Art 38)

3. The controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks

6. The DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests

Publication (Art 37)

7. The controller or the processor shall publish the contact details of the DPO and communicate them to the [UK] Commissioner / [EU] supervisory authority

UK DPDI Bill

Conflicts (Art 27B)

5 Where the performance of one of its tasks would result in a conflict of interests, the SRI must secure that the task is performed by another person

6. In deciding whether one or more of their tasks should be performed by another person (whether alone or jointly with others) and, if so, by whom, the SRI must consider, among other things: ...

(c) whether the other person is involved in day-to-day processing of personal data for the controller or processor and, if so, whether that affects the person's ability to perform the task

Art 27(C)

2. A controller or processor must not dismiss or penalise its SRI for performing the individual's tasks

3. Where the SRI decides that one or more of its tasks should be performed by another person, the controller or processor must ensure that the person: ...

(b) is not dismissed or penalised by the controller or processor for performing the task, and

(c) does not receive instructions about the performance of the task

4. Paragraph 3(c) does not require the controller or processor to prevent instructions being given by the SRI or another person performing a task for the SRI, except where such instructions would involve a conflict of interests

Publication (Art 27)

4. The controller or processor must:

(a) ensure that the current contact details of the SRI are publicly available, and

(b) send those details to the Commissioner

DPIAs & Assessments

DPIAs

UK & EU GDPR

Data protection impact assessment (Arts 35 & 57)

When required

35(1). Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of **natural persons**, the **CONTROLLER** shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

35(3). A DPIA referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person

(b) processing on a large scale of special categories of data referred to in Art 9(1), or of personal data relating to criminal convictions and offences referred to in Art 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale

Supervisory Authority Lists

37(4) & (5). The [UK] Commissioner / [EU] supervisory authority shall establish and make public a list of the kind of processing operations which require a DPIA and may publish a list that are not. [EU] The supervisory authority shall communicate those lists to the EDPB and apply the consistency mechanism

57(1). Without prejudice to other tasks set out under this Regulation, the Commissioner must / each supervisory authority shall on its territory: …

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4)

UK DPDI Bill

Assessment of high risk processing (Art 35)

When required

35(1). Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of **individuals**, the **CONTROLLER** shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

[deleted]

Supervisory Authority Lists

[deleted, though Art 35(6) is not deleted and it relies on 35(4) and (5). Perhaps this will be corrected before enactment.]

57(1). Without prejudice to other tasks set out under this Regulation, the Commissioner must: …

(k) produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals (for the purposes of Articles 27A, 30A and 35)

DPIAs

UK & EU GDPR

Data protection impact assessment (Art 35)

Content

7. The assessment shall contain at least:

Processing: description & purposes
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller

Necessity & proportionality
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes

Risk assessment
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

Risk measures
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned

UK DPDI Bill

Assessment of high risk processing (Art 35)

Content

7. The **CONTROLLER** must produce a document recording compliance with this Article which includes at least:

Processing: purposes
(a) a summary of the purposes of the processing

Necessity
(b) an assessment of whether the processing is necessary for those purposes

Risk assessment
(c) an assessment of the risks to individuals referred to in paragraph 1, and

Risk measures
(d) a description of how the controller proposes to mitigate those risks

DPIAs

UK & EU GDPR

Data protection impact assessment (Arts 35 & 36)

Advice

35(2). The **CONTROLLER** shall seek the advice of the DPO, where designated, when carrying out a DPIA

Consultation

35(9) Where appropriate, the controller **shall** seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations

36(1) The controller **shall** consult the [UK] Commissioner / [EU] supervisory authority prior to processing where a DPIA under Art 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk

Review

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations

UK DPDI Bill

Assessment of high risk processing (Art 35 & 36)

Advice

[deleted]

Consultation

[deleted]

Art 36(1) The controller **may** consult the Commissioner prior to processing where an assessment under Art 35 indicates that the processing would result in a high risk to the rights and freedoms of individuals in the absence of measures taken by the controller to mitigate the risk

Review

11. The controller shall carry out a review of an assessment pursuant to paragraph 1 where necessary and at least when there is a change of the risk represented by processing operations

DSRs

DSRs

UK & EU GDPR

Data subjects' rights (Art 12)

Charging or refusing

12(5). Information provided under Arts 13 and 14 and any communication and any actions taken under Arts 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are **manifestly unfounded** or **excessive**, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request

UK DPDI Bill

Data subjects' rights (Art 12 & Art 12A)

Charging or refusing

12(5). Information provided under Arts 13 and 14 and any communication and any actions taken under Arts 15 to 22 and 34 shall be provided free of charge. [rest of 12(5) deleted]

12A(1). Paragraph 2 applies where a request from a data subject under any of Arts 15 to 22 or 34 is **vexatious** or **excessive**

12A(2). The controller may:

(a) charge a reasonable fee for dealing with the request (see s12, UK DPA 2018), or

(b) refuse to act on the request

'Vexatious or excessive'

12A(4). Whether a request is vexatious or excessive must be determined having regard to the circumstances of the request, including (so far as relevant):

(a) the nature of the request

(b) the relationship between the data subject and the controller

(c) the resources available to the controller

(d) the extent to which the request repeats a previous request made by the data subject to the controller

(e) how long ago any previous request was made, and

(f) whether the request overlaps with other requests made by the data subject to the controller

12A(5). Examples of requests that may be vexatious include requests that:

(a) are intended to cause distress

(b) are not made in good faith, or

(c) are an abuse of process

A few takeaways

Hey, that's just another apple!

To us:

- RoPAs are essentially the same under both,
- obligations on SRIs are far greater than on DPOs (and the conflict rule remains, something we'd like to see go),
- obligations on risk assessments potentially apply in broader scenarios than in GDPR, and require similar effort, and
- DSRs are unchanged (changing *manifestly unfounded* to *vexatious* is unlikely to have a significant impact in practice).

High risk?

Much of DPDI's changes, that affect Privacy in practice, depend on the words '*likely to result in high risk*' or '*high risk*'. This comes into play on the SRI, risk assessments and RoPAs.

But what does it mean? Or, rather, when is it calculated?

- ❑ If it's **inherent** risk, then **everyone** needs an SRI, to carry out a number of risk assessments, and keep an extensive RoPA.

- ❑ If it's **residual** risk, then **practically no-one** will need an SRI, do a risk assessment or keep a RoPA.

That's because, under GDPR, you're not meant to carry out high risk processing without consulting the regulator to try to reduce the risk.

If DPDI is to maintain levels of data protection, then this principle surely needs to remain. And it's unlikely that either result above is the government's intent. More certainty is needed here.

Does proportionality still matter?

'Necessary and proportionate' is a common yardstick in data protection law and it's set out in GDPR for DPIAs.

The Bill removes proportionality from assessments, where DPDI just talks about necessity. Is that a typo or is the intent to ignore proportionality?

A word on processors

The idea that a processor can 'get away with' less compliance is mostly a fallacy.

They may be a processor to customers, but they're a controller for all their own HR, Finance, Legal, Sales, Marketing, IT and more. They have employees, directors, suppliers, partners and shareholders.

So, for the vast majority of organisations, it's a case of 'controller + processor'.

Keepabl™
PRIVACY
SECURITY
COMPLIANCE

hello@keepabl.com

Do visit us at keepabl.com

Struggling to know where to start? Is your RoPA unmanageable, strung out over various spreadsheets?

Time to automate! You use SaaS for HR, Finance and Sales for a reason.

- ✓ See why one consultant believes **we save his clients between 50% and 70% on ongoing Privacy governance**.
- ✓ Or why listed wealth manager Canaccord Genuity UK & Europe says: '*We're delighted to have **a solution that has such a positive effect on how we work** and meet ongoing GDPR compliance across countries.*'
- ✓ Or why investor MML Capital says: '*Keepabl's Dashboard helpfully visualises our GDPR KPIs. We can give stakeholders tailored access, and we can work more efficiently with our external advisers.* ***All this saves me lots of time – and stress!***'

2022 REGTECH 100
2021 REGTECH 100
2023 REGTECH 100

Keepabl named to the RegTech100 three years running!

'The world's most innovative RegTech companies that every leader in the regulatory industry needs to know about'