Reporting on GDPR Compliance

An Accountability Approach to GDPR Regulator Ready Reporting
Contents
Introduction ................................................................................................................................................................. 3
Regulator Ready Reporting - Approach .......................................................................................................................... 4
Minimum Compliance Requirements .............................................................................................................................. 5
  Regulator Ready reporting on enterprise level technical and organisational measures (Article 24 and 5) .............................................................. 6
  Regulator Ready reporting on records of processing (Article 30): ............................................................................. 8
  Regulator Ready reporting on data protection impact assessments (DPIA) (Article 35) .............................................. 9
Additional Accountability Reporting ......................................................................................................................................... 11
  Regulator Ready Reporting on data protection by design (Article 25) ....................................................................... 11
  Regulator Ready Reporting on Legitimate Interests as lawful basis for processing (Article 6(1)(f) ...... 13
Conclusion............................................................................................................................................................................ 14
Introduction

What is Regulator Ready reporting and why do you need it?

Regulator Ready reporting means you have the capacity to efficiently generate required reports that clearly tell a story reflecting your organisation’s GDPR compliance and accountability.

To understand the growing need for Regulator Ready reporting, imagine the following scenarios.

- In the first situation, your organisation experiences a breach. Within a short period of time, and reactively, the Regulator is on your doorstep.
- In a second scenario, your organisation has not had a breach or any other public privacy incident, but the Regulator comes knocking at your door, expecting to assess your organisations GDPR compliance.
- In the final scenario, you may be launching a new product or service that has privacy implications. Your organisation initiates a meeting with the Regulator to provide assurance that not only is your product GDPR compliant but that you have considered privacy by design in the product itself as well as embedded it throughout your organisation.

In any of these scenarios, you want to be able to deliver “Regulator Ready” reporting.

Many regulators prefer voluntary compliance but are prepared to back that up with tough action when required. And if that happens, expect that the Regulators will be tough. Organisations had two years to prepare for GDPR compliance in the run-up to the applicability date of May 25, 2018. So, what will the Regulator want to see and how can you be “Regulator Ready”?

---

1 Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2 “The aim of the GDPR is to prevent harm, and we place support and compliance at the heart of our regulatory action. Voluntary compliance is still the preferred route, but we will back that up with tough action where it’s necessary” [https://iapp.org/news/a/icos-denham-may-25-is-not-doomsday/#](https://iapp.org/news/a/icos-denham-may-25-is-not-doomsday/#)
Regulator Ready Reporting - Approach

Demonstrating compliance to Regulators is an important pillar of the GDPR and organisations need to be ready to report on this compliance\(^3\) and be able to provide on demand explanations of their privacy program, including procedures and the underlying decisions.

There are three main components to Regulator Ready Reporting:

1. **Accountability is the cornerstone**
   - Articles 5, 24 (demonstrate compliance and put in place appropriate technical and organisational measures)

2. **Leverage existing measures and accountability mechanisms and embed into projects to meet additional compliance requirements:**
   - Article 30 – records of processing activities
   - Article 35 – data protection impact assessments
   - Article 25 – data protection by design
   - Article 6(1)(f) – assessment to show legitimate interests as lawful basis for processing

3. **Generate reports that tell your organisations accountability and compliance story**

The accountability principle in Article 5(2) requires organisations to demonstrate compliance with the principles of the GDPR. Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures to ensure that organisations can demonstrate that the processing of personal data is performed in accordance with the GDPR. To demonstrate compliance with Article 5(2) and 24 organisations need a way of presenting their appropriate technical and organisational measures in a structured format. Some organisations go far beyond what is legally required for compliance in the GDPR and also document technical and organisational measures that have been put in place to further enhance accountability throughout their organisation.

Organisations that prepare for Regulatory Ready reporting leverage the technical and organisational measures that are currently in place to embed accountability into projects allowing them to efficiently generate reports for multiple compliance requirements (Records of Processing, DPIAs, legitimate interests assessments and more). For example, when new projects are initiated, the privacy office often requires that the operational unit complete a “threshold PIA.” A threshold PIA pre-emptively detects an organisation’s use of personal data, which, if identified, would require subsequent PIAs. If done correctly, the threshold PIA can collect all the data necessary for Article 30 (records of processing) reports.

In addition, a threshold PIA can identify if the processing is likely to be high risk and require a data protection impact assessment as required under Article 35. In a Regulator Ready reporting approach, organisations that are processing high risk data will use their data protection impact assessment method to embed appropriate technical and organisational measures directly into the project and require

---

\(^3\) Both Articles 5 and 24 contain explicit references to this principle. Article 5 – the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability) | Article 24 – (…) the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.
evidence that the business or operational unit is applying the measures. Thus, the technical and organisational measures become the cornerstone of the DPIA report. The measures are applied prior to processing the data which reduces risk.

Next, because the organisation has embedded appropriate technical and organisational measures directly into the data protection impact assessment, the project itself is now designed with privacy and data protection in mind. So the organisation can easily generate a DPbD or PbD report.

Finally, this Regulator Ready approach can also help with producing the necessary information when some organisation chooses to rely on legitimate interests as a lawful basis for processing. Courts and Regulators had indicated that the more safeguards that are in place (technical and organisational measures) the more likely the balance will tip in favor of the controller.\(^4\)

In summary, a “Regulator Ready reporting” approach to compliance means effectively operationalizing the use of appropriate technical and organisational measures to allow for reporting on:

- Demonstrating compliance (Article 5(2) and 24)
- Records of processing (Article 30)
- Data Protection Impact Assessments (Article 35)
- Data Protection by Design (Article 25)
- Using legitimate interests as a lawful basis for processing (Article 6(1)(f))

---

This is Regulator Ready reporting which can be used to demonstrate compliance with the required compliance elements or beyond by showing additional accountability elements.

---

**Minimum Compliance Requirements**

When a Regulator comes knocking they will want to see evidence of key requirements. The following Articles under the GDPR specifically indicate that documentation of some type must be made available, to supervisory authorities.

1. **Article 5.2 Accountability and Article 24 Responsibility of the Controller:** The need to be accountable and to demonstrate compliance is codified in the GDPR in Article 24, which closely links to Article 5 on the data protection principles. At a minimum, they would need a

---

\(^4\) Reference Nymity and FPF Legitimate Interest report
demonstration of the appropriate technical and organisational measures that have been put in place at an organisational level.

2. **Article 30 Records of Processing Activities**\(^5\) requires that controllers and processors must maintain a record of processing activities and make the record available to the supervisory authority on request. At a minimum, regulators will want to see a record of processing for all processing occurring prior to May 25, 2018 and records for any new processing that occurred after that date.

3. **Article 35 Data Protection Impact Assessment (DPIA)**\(^6\) requires that controllers carry out DPIAs in high risk processing scenarios and at a minimum the Regulator will want to see a DPIA report for any new processing or major changes to current processing post May 25th.

### What does “Regulator Ready reporting” look like for these three requirements elements?

**Regulator Ready reporting on enterprise level technical and organisational measures (Article 24 and 5)**

As referenced above, Article 5(2) of the GDPR contains an explicit provision regarding documenting your compliance with all the principles related to the processing of personal data. Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures. Therefore, in addition to records of processing and DPIAs, documentation must be kept reflecting other aspects of your compliance with the GDPR including:

- Privacy Notices
- Consent forms and evidence of consents
- Procedures for the exercise of individual rights
- Processor agreements
- Breach response implemented
- Controller-processor contracts
- Internal procedures in the event of a data breach
- Data transfer mechanisms (e.g., EU Model Clauses, Binding Corporate Rules and certifications, where applicable) etc.

The measures and associated documentation with your compliance program must be regularly re-examined and updated to ensure continued data protection. There is no specific guidance respecting how to report on your enterprise level compliance. However, being “Regulator Ready” to report at an

---

\(^5\) Article 30(4) The controller or the processor and, where applicable, the controller’s or the processor’s representative, shall make the record available to the supervisory authority on request.

\(^6\) Article 35 (1) Where at 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...
enterprise level means that you have a good understanding of which obligations under the GDPR apply to you, that you have addressed compliance respecting those obligations throughout the organisation and that you have evidence of this compliance.

To assist organisations in being able to report on GDPR compliance at an enterprise level, Nymity Research™ identified 39 Articles under the GDPR that require evidence of a technical or organisational measure to demonstrate compliance and mapped those to the Nymity Privacy Management Accountability Framework™. Nymity provides several free resources that assist organisations in understanding their GDPR obligations and prioritizing compliance.

An example of a “Regulator Ready” report could be a spreadsheet or word document that ties the relevant provisions of the law to the technical and organisational measures that have been put in place and are being maintained for GDPR compliance. For example, the measure “document legal basis for processing personal data” would be tied to Article 6 which deals with the lawfulness of processing. Next, for each of the measures that is maintained, the report would contain the evidence collection question(s) that are used within the organisation as well as the answers and comments that have been added by the owner(s) of the measure. Finally, the report would contain a reference to the owner of each activity and the comments (s) he has added to the question as well as the date when the information was updated. A report like this could be a quick overview of the overall status of the organisation’s privacy program and the underlying evidence to support it. (see example below)

Another way of demonstrating compliance could be with a “scorecard: This scorecard could also present evidence of technical and organisation measures that have been implemented that go beyond the legal requirements of the GDPR. A scorecard provides you Regulator Ready Reporting.

Sample spreadsheet documenting GDPR capacity to comply

<table>
<thead>
<tr>
<th>Art.</th>
<th>Art. Title</th>
<th>Appropriate Technical or Organisational Measures</th>
<th>Privacy Office Evidence Collection Question</th>
<th>Comments</th>
<th>Evidence of Accountability Mechanism</th>
<th>Owner and Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Lawfulness of processing</td>
<td>Document legal basis for processing personal data</td>
<td>Have you identified general categories of data, processing activities, and the legal basis under which they are carried out?</td>
<td>The existing log that records the legal basis for processing personal data has now been updated to include special categories as identified under the GDPR indicating how determinations were made.</td>
<td>Master Sensitive Data Processing Log Record</td>
<td>Mr. Rooz 6/30/2016</td>
</tr>
<tr>
<td>7</td>
<td>Conditions for consent</td>
<td>Maintain procedures to respond to requests to opt-out of, restrict or object to processing</td>
<td>Is there a mechanism for data subjects to withdraw consent, and have you reviewed it to determine if it is straightforward and timely?</td>
<td>The procedures for responding to data subject requests to withdraw consent have been reviewed and were found to be current.</td>
<td>intranet.com/Privacy/VS Manual</td>
<td>Mr. Rooz 6/30/2016</td>
</tr>
<tr>
<td>8</td>
<td>Conditions applicable to child’s consent in relation to information</td>
<td>Maintain policies/procedures for obtaining valid consent</td>
<td>Do you review consent mechanisms/requests for consent for prominence, accessibility and simplicity?</td>
<td>The procedures for responding to data subject requests to withdraw consent have been reviewed and were found to be current.</td>
<td>Web forms, signed consent forms and call-center recordings are scheduled to be reviewed in Q2</td>
<td>Mr. Rooz 3/30/2017</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintain policies/procedures for obtaining valid consent</td>
<td>Integrate data privacy into the organization’s use of social</td>
<td>We do not offer information services directly to children.</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

7 Nymity GDPR toolkit

© 2018 Nymity Inc. www.nymity.com
Regulator Ready reporting on records of processing (Article 30):
A requirement of the EU Data Protection Directive 95/46/EC (“Directive”) was to notify and register processing activities with local DPAs. Article 30 replaces this requirement and requires organisations to make a record of processing activities⁸ available to the supervisory authority on request.

In general, the record must document the following information:

- The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer).
- The purposes of your processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

⁸ The requirement does not apply where the controller employs fewer than 250 persons and the processing is not likely result in a risk for the rights and freedoms of data subjects, is occasional, or is not of special categories of data). And, for a detailed discussion on how a record of processing activities differs from a traditional data inventory, see Nymity publication, "Does GDPR Article 30 require a Data Inventory" found at https://info.nymity.com/hubfs/GDPR%20Resources/Nymity_Insights-GDPR_Article_30_Data_Inventory.pdf?ut=1528467028689
Under the former Directive, the requirements varied by country with some countries requiring more information than others, but organisations compliant with this requirement, have the information readily on hand and it should not be that difficult to pull together the Article 30 record rather quickly. For those who don’t, they will find that the process of putting together this record aligns well with how the business processes data because it starts by listing the processing activities and their purpose. This makes it easy for the business to engage and the Privacy Office to get more and better data and thus the GDPR has created an opportunity for organisations to limit their data inventory to an inventory of their data processing operations of that is what they choose. And, documenting your processing activities is important, not only because it is itself a legal requirement, but it can help you demonstrate your compliance with other aspects of the GDPR.

What does a “Regulator Ready” report of a records of processing activities look like? The GDPR specifies the required elements for a record of processing but does not specify what a record should look like. A few supervisory authorities have issued local guidance and sample templates in either in excel or word format9 and below is a sample image of a “Regulator Ready” Article 30 report generated from Nymity ExpertPIA™ Solution.

Regulator Ready reporting on data protection impact assessments (DPIA) (Article 35)
As mentioned above, Article 35 of the GDPR requires that controllers carry out DPIAs in high risk processing scenarios. If the Regulator comes knocking at your door due to a breach or expecting to inquire about your program, at a minimum the Regulator will want to see a DPIA report for any new processing or major changes to current processing post May 25th.

An Article 35 “Regulator Ready” DPIA Report tells the legal story of risk mitigation, which is the mandate found in Article 35. While some supervisory authorities have provided examples of templates10 to use in such an assessment, it is clear that what is important is to document an organisation’s decision making11. The traditional approach PIAs is a questionnaire form. This format has proven over time to have many challenges including they are resource intensive for the Privacy Office/DPO; business units are not generally motivated to take ownership of the process or complete the PIA; the advice provided ages quickly; they present a

10 See for example sample template from UK ICO found at https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf
standard and inflexible methodology; PIAs are not reviewed for effectiveness, documenting gaps creates legal risk and, unnecessary resources are used for similar processing projects.

An alternative approach to documenting DPIA determinations is to clearly tell the story of how risk was mitigated in the project and its effectiveness. Whatever form is used, the below content and categories will document and narrate a defensible position regarding a DPIA assessment:

- What GDPR DPIA Criteria made the process likely to be high risk
- What are the purposes of processing (this can be leveraged from the record of processing activities)
- What potential benefits are provided to the data subjects
- What risks to processing the personal data have been mitigated
- What risk of harm to the data subject have been mitigated
- How the risk was mitigated (by identifying the appropriate technical and organisational Measures)
  - How we know the risk was mitigated effectively (by adding privacy by design effectiveness questions)
  - How the business has affirmed their accountability for addressing the risk (through affirmations and additional notes)

The report could also include additional information such as data transfer mechanisms, data types, data subjects, data recipients, records retention, location of data collection and location of data processing -- all factors that helped in the assessment that determined the likely high risk for the project.
From an accountability standpoint, it may also be beneficial to report on compliance with other key provisions of the GDPR:

1. **Article 25 - Data Protection by Design/Default** where applicable: From an accountability standpoint it may be beneficial to show who the appropriate technical and organisational measures are applied at a processing level.

2. **Article 6 (1)(f) – Legitimate Interests as lawful basis for processing:** The GDPR sets practical and clear criteria for organisations that seek to rely on legitimate interests as a lawful ground for processing personal data but organisations must document their decision making and be able to report on it to a supervisory authority.

**Regulator Ready Reporting on Data Protection by Design (Article 25)**

Article 25 requires that controllers shall, at the time the determination of the means for processing as well as at the time of processing itself, implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement the data protection principles as well as integrate the necessary safeguards into the processing.
When creating a new project or service, many organisations conduct a privacy impact assessment or something similar even when a legally mandated DPIA is not required. Whether a DPIA or a more general privacy impact assessment, the organisation documents the appropriate technical and organisational measures that it used and is maintaining to ensure appropriate data protection in relation to the processing. This information can be collated to produce a Regulator Ready” Data Protection by Design report. The key elements of such a report would include:

- A list of the appropriate technical and organisational measures
- A description of the measures
- Affirmations that the Measures are being used
- Additional Affirmational comments.

While such a report is simple in nature, it is a powerful reporting tool for an organisation as it demonstrates to the regulator that privacy is embedded in the design of the product or service.

An example report may look like the following:

<table>
<thead>
<tr>
<th>Question</th>
<th>Affirmation</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facial Recognition. From section 2.4 of the Employee Monitoring Policy, did you address that the company will not use facial recognition technologies or audits?</td>
<td>Yes</td>
<td>The facial recognition/facial recognition was necessary</td>
</tr>
<tr>
<td>CCTV Notice: from section 3.6 of the Employee Monitoring Policy, did you address that the company will notify employees when they are entering an area being monitored?</td>
<td>Yes</td>
<td>We used the standard notices that are placed under remotes.</td>
</tr>
<tr>
<td>Individual Rights Policy. Are individuals provided the right to object to the processing based on legitimate interests?</td>
<td>Yes</td>
<td>Yes. An opt-out is provided on website privacy policy found at <a href="http://www.abcc.ca">www.abcc.ca</a></td>
</tr>
<tr>
<td>Privacy Notice: Does the privacy notice identify the legitimate interests? The legal grounds for processing?</td>
<td>Yes</td>
<td>Details are included on website privacy policy found at <a href="http://www.store.com">www.store.com</a></td>
</tr>
</tbody>
</table>
Regulator Ready Reporting on Legitimate Interests as lawful basis for processing (Article 6(1)(f))

The GDPR Article 6(1)(f) sets practical and clear criteria for organisations that seek to rely on legitimate interests as a lawful ground for processing personal data. These include:

1. Identify a legitimate interest;
2. Show that the processing is necessary to achieve it; and
3. Balance it against the individual’s interests, rights and freedoms.

A Regulator Ready report first identifies the legitimate interest for the processing and whether or not the processing is necessary to achieve that interest. However, the mere existence of a sufficiently articulated legitimate interest is not enough for the processing to be considered lawful. The processing must also be “necessary” for those legitimate interests. And, the final element to be complied with is the balancing exercise between those interests and the interests of the individuals whose data are processed. To help determine this balancing exercise, a Regulator Ready report can include the following elements:

- a) the individuals that are impacted by the processing (data subject categories);
- b) the potential harms to individuals that have been mitigated by the use of appropriate safeguards (Potential Harms to Individuals Mitigated);
- c) the processing risks that have been mitigated by the use of appropriate safeguards (Processing Risks Mitigated);
- d) the Accountability Mechanisms that have been put in place to address the potential harms and risks (safeguards).

Finally, an “Approver” must make a final determination. If the Approver is satisfied that the three criteria are met, legitimate interest will ensure you won’t have to rely upon consent, making your processing operations more future proof.

Historically there has been very little guidance on how to conduct an assessment respecting legitimate interest. Recently, the UK ICO released guidance 12 and a sample template for conducting a legitimate interest assessment (LIA). When completed, such a template could serve as a “Regulator Ready” report should a supervisory authority request evidence respecting an organisation’s use of legitimate interests as a lawful ground for processing.

---

Conclusion

As noted above, demonstrating compliance to Regulators is an important pillar of the GDPR and organisations need to be ready to report on this compliance and be able to provide on demand explanations of their privacy program, including procedures and the underlying decisions. The cornerstone of a Regulator Ready Reporting is Accountability.

When accountability is in place, organisations can leverage existing technical and organisational measures and embed them at the project level and ultimately produce a variety of reports to demonstrate accountability and compliance to regulators, on demand.