GDPR Current Market – 907.4 Million $

Expected Market Growth – 2659.4 Million $

Information About the Market –

The GDPR market comprises of 2 scenarios – Solution Market (Data discovery and Mapping, Data Governance, and API Management), and Service Market (GDPR Readiness Assessment, Risk Assessment and DPIA).

Note that the above information is not specific to DPIA, but other data protection services as well.

Source -- <https://markets.businessinsider.com/news/stocks/gdpr-services-market-worth-2-659-4-million-usd-by-2023-1027344200> [1]

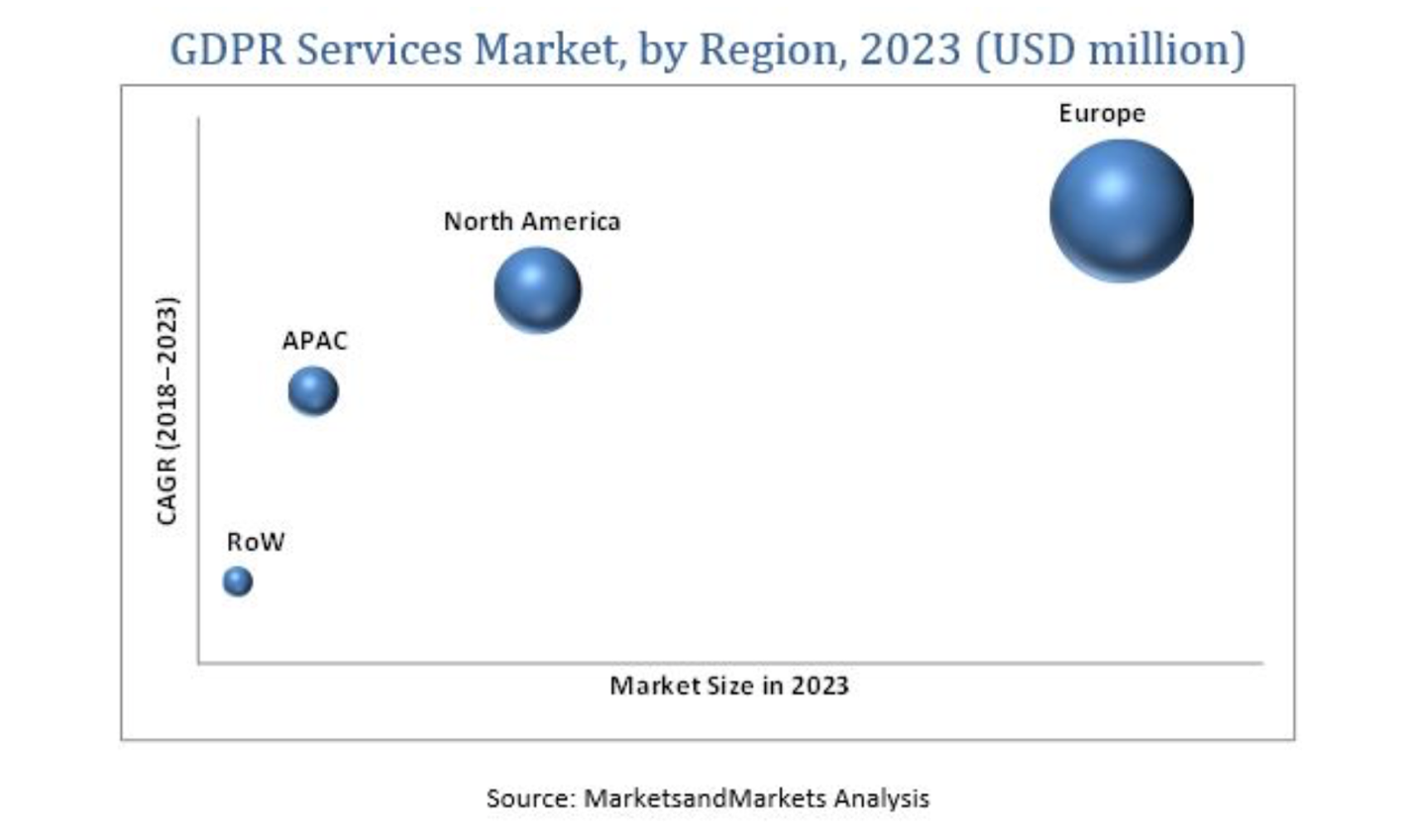
<https://www.marketsandmarkets.com/Market-Reports/gdpr-services-market-187994915.html> [2]

Some of the market expectations –

1. Large enterprise segment expected to account for a larger market share as compared to the SME segment during the forecast period. However, all the large LME were expected to become GDPR complaint by May 2018 as they had more to lose by not becoming GDPR compliant. Therefore, in the future, the target should be to acquire small scale companies. [1]
2. Major vendors covered in the **GDPR Services Market** (This is DPIA specific since DPIA forms major part of ***GDPR Services Market***)include Absolute Software (Canada), Actiance (US), AWS (US), Capgemini (France), Hitachi Systems Security (Canada), IBM (US), Informatica (US), MetricStream (US), Micro Focus (UK),  Microsoft (US), Mimecast (UK), Nymity (Canada), OneTrust (US and UK), Oracle (US), Proofpoint (US), Protegrity (US), SAP (Germany), SAS (US), Snow Software (Sweden), Swascan (Italy), Symantec (US), Talend (US), TrustArc (US), Trustwave (US), Varonis (US), and Veritas (US). [1]

Key Target Audience [2]

* Data Subjects
* Data Controllers
* Data Processors
* Data Protection Officers
* GDPR Services Solution Providers
* GDPR Services Service Providers
* Government Organizations



APAC – Asia Pacific

RoW – Rest of World

OneTrust simplifies and operationalises this process by enabling you to execute 4 simple

steps:

1. Design and Build a Questionnaire, or use OneTrust’s pre-built DPIA template

2. Launch and Collect Responses

3. Enforce and Remediate Risks

4. Analyze & Report on Results

Note – This Questionnaire can be modified on the business needs and requirements.

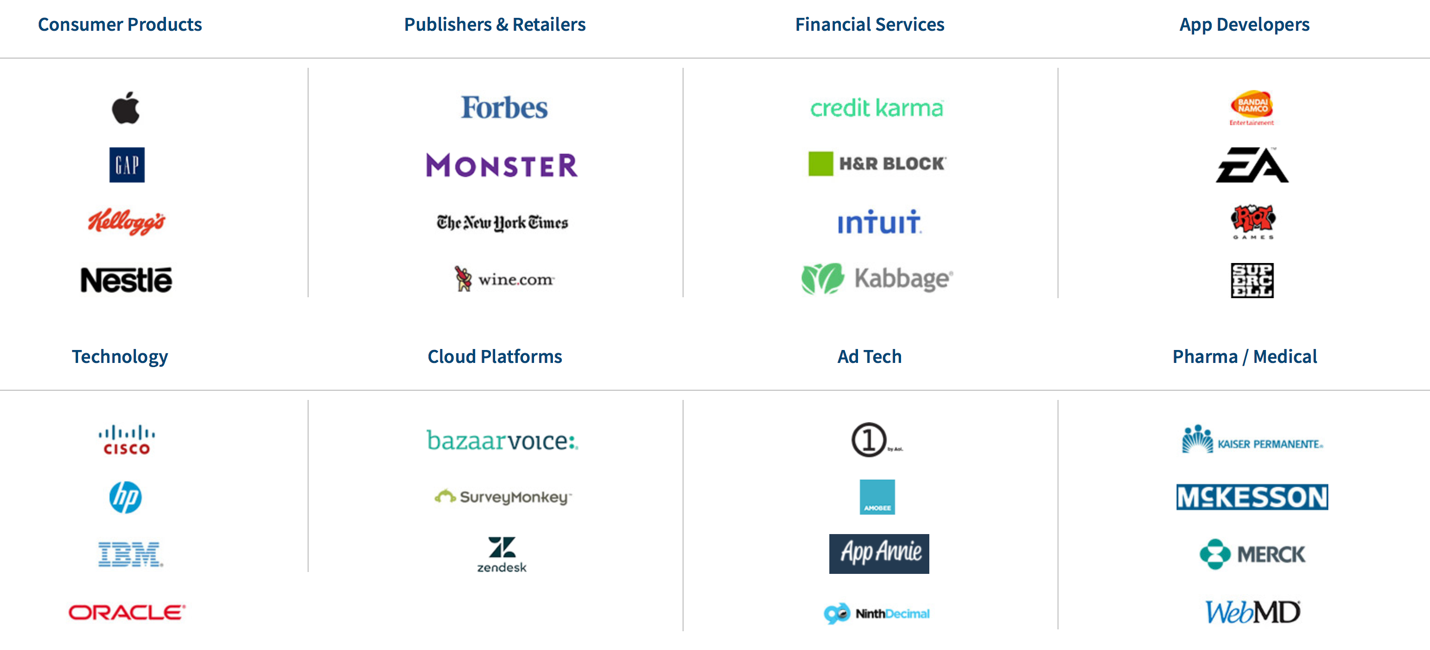
Source – [www.onetrust.com](http://www.onetrust.com) (Erik’s white book)

The document is quite detailed and lists 10 types of processing activities subject to the requirement for a DPIA:

1. Evaluation and assessment, including profiling and forecasting (behavioral analysis) for purposes which may cause negative legal, physical, financial or other consequences/inconvenience for natural persons.
2. Automated decision-making that produces legal, financial or similar significant effects.
3. Systematic monitoring on a large scale of publicly available places, which uses elements of recognition of features or characteristics of facilities located within the monitored area. This group does not include CCTV where the picture is recorded and used only to analyze breach of law incidents.
4. Processing of special categories of personal data and of personal data relating to criminal convictions and offences (sensitive data according to Article 29 Data Protection Working Party guidelines).
5. Data processed on a large scale where the term “large scale” refers to the number of persons whose data is processed; scope of processing; retention period; geographical scope of processing.
6. Conducting comparisons, assessments and drawing conclusions, based on the analysis of data acquired from different sources.
7. Processing personal data of persons whose assessment and services rendered are conditional on subjects and persons who have supervisory and/or evaluating powers
8. Innovative use or application of technological or organizational solutions.
9. Transfer of personal data outside the EU.
10. Where data processing in itself “makes it impossible for persons whose data is processed to exercise his/her right or use a service or an agreement.”

**Trust Arc Process –**

1. Define Roles and Responsibility
2. Create Process workflow
3. Assessment Content – Same modifiable questionnaire
4. Implement scalable program



Source -- <https://www.trustarc.com/customer-success/>

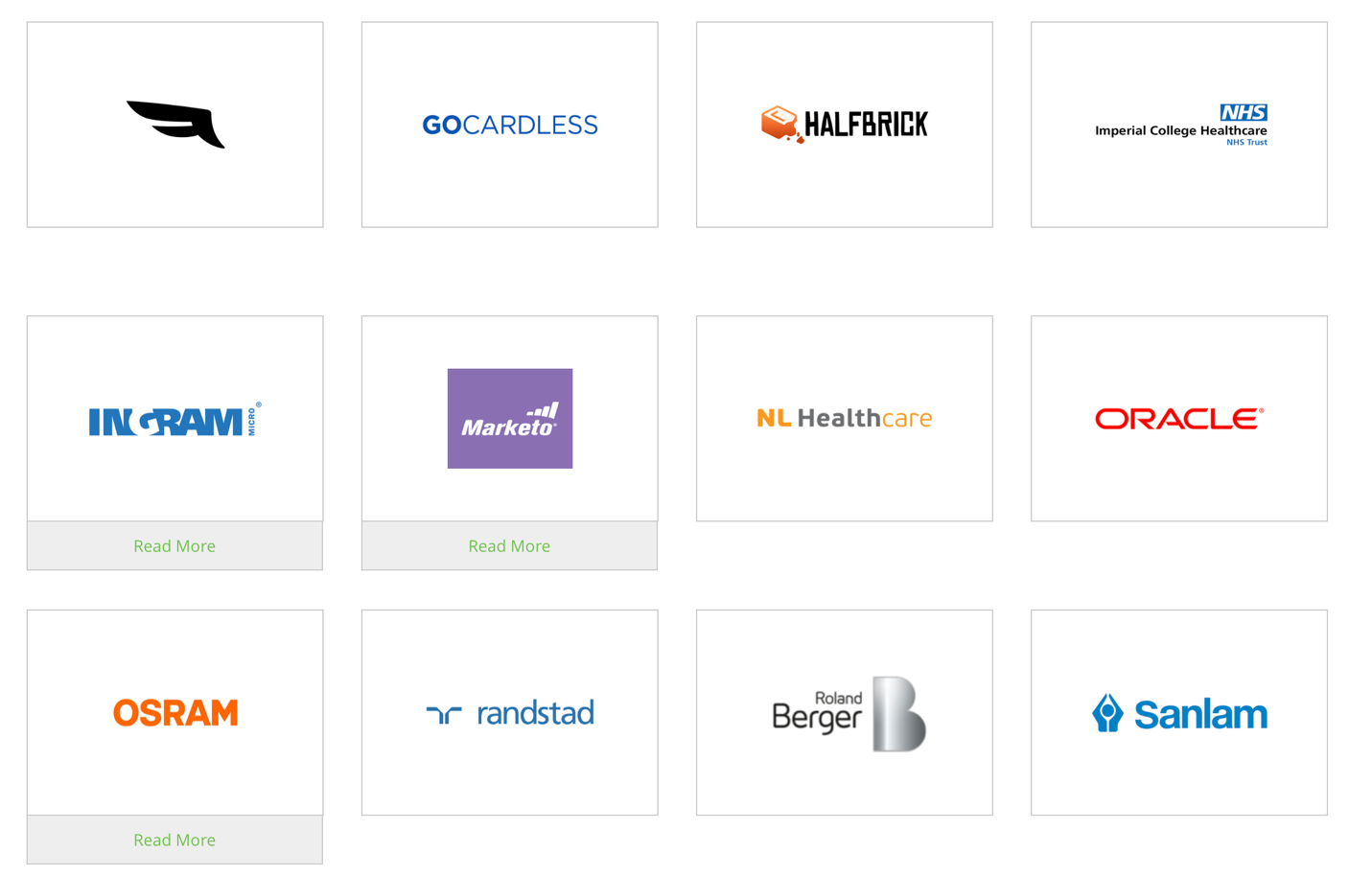
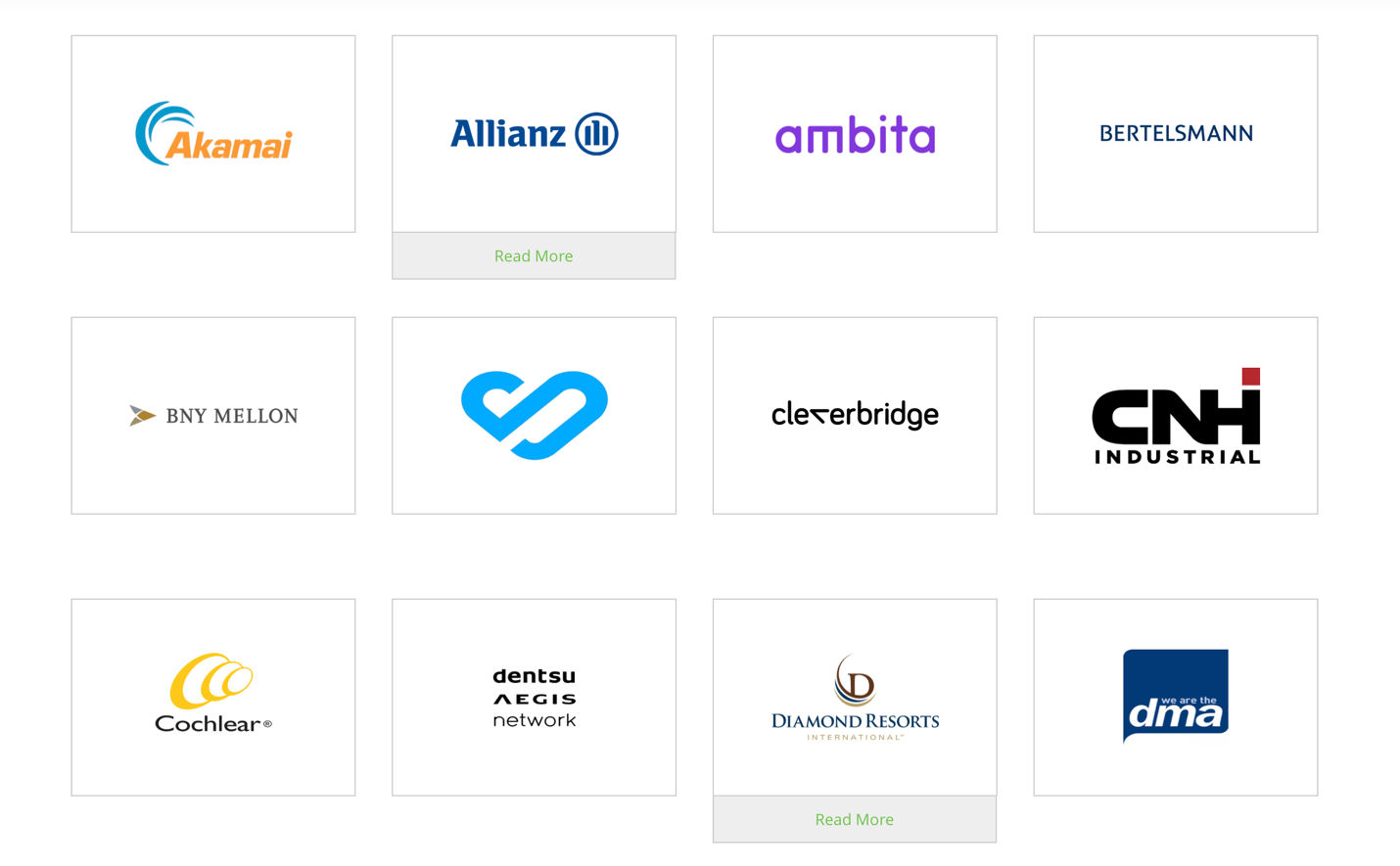
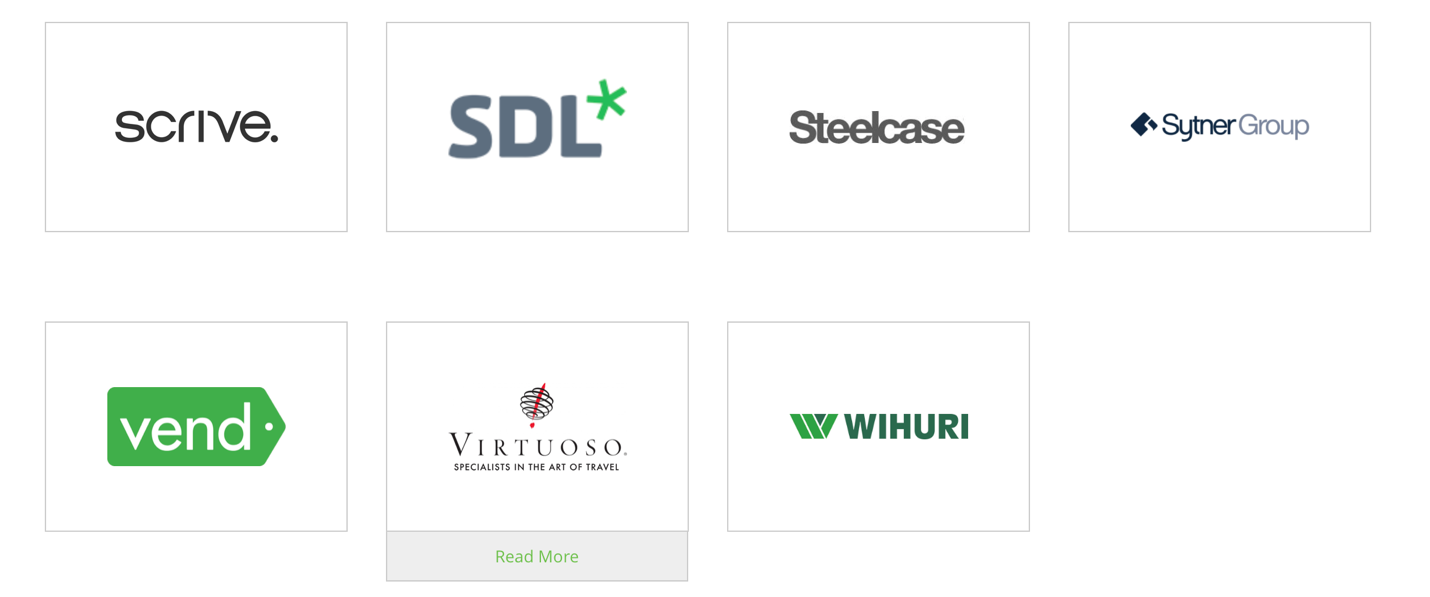
**Trust Arc Competitive Advantage –**

1. Extensive Logic Based Workflows
2. Accountability with Reporting Features – Advantage for creating Article 30 reports
3. Unique combination of Technology + Expertise
4. A more holistic privacy program

Source -- <https://download.trustarc.com/dload.php/?f=52GRN7BR-691>

**One Trust Customers –**

Source -- <https://www.onetrust.com/customers/>



**Other Alternatives –**

**Trust wave and veritas – not much found – They are in the GDPR market, but do not have specific DPIA’s respectively.**

**Capgemini –**

Process – DPIA through Data Subject Consultation

A few of the consultation mechanisms that can be considered are focus groups, user groups, public meetings, consumer panels, town hall meetings, individual interviews, paired interviews, and surveys – depending on the type and nature of processing.

To this end, here are some logical steps to help you set up a solid consultation process with your data subjects:

* Design a consultation process and create guidelines for the process.
* Develop a communication and response gathering strategy.
* Provide your data subjects with adequate information about the project in a clear manner for them to make valid contributions; explain what the process will be, why the consultation is being undertaken, how long it will last, what are the expected results, and how they will be used.
* Document the reasons, in the event your data controller’s final decision differs from the views of the data subject.
* Document the justification with clear explanations for not seeking the views of the data subject, in the event your data controller decides the data subject’s consultation isn’t appropriate.

 The benefits of data subject consultation

Consulting data subjects or their representatives enables your organization to:

* Assess the risk to your data subjects’ rights and freedoms, and identify measures to reduce risk to an acceptable level.
* Demonstrate compliance with GDPR requirements.
* Foster greater trust and confidence of your data subjects and data controllers.
* Benefit from options based on a wider range of views gathered.
* Identify risks related to significant social or economic disadvantage.
* Improve understanding of your data subjects’ needs, concerns, and expectations.
* Avoid potential reputational damage at a later stage.

To conclude, consulting data subjects enhances the effectiveness of your DPIA process, which helps to ensure GDPR compliance. In the absence of a data subject consultation process, it is strongly advised that you document the reasons for not consulting your data subjects, with valid reasons to help you demonstrate compliance if challenged.

**Understanding – Mostly the same DPIA process**

**Clients – Yet to figure out !**

**Source -- https://www.capgemini.com/2018/04/dpia-under-gdpr-consult-your-data-subjects/**