



2nd Edition, March 2018

# Organisational Readiness for the European Union General Data Protection Regulation (GDPR)



# Table of Contents

Foreword .....	3
Executive Summary.....	4
Survey Results and Key Findings.....	7
1. GDPR Impact, Organisational Readiness & Resources .....	7
1.1 Key Areas of Impact .....	7
1.2 Top Areas of Senior Management Concerns .....	8
1.3 Readiness for Change.....	9
1.4 Impact on Resources.....	10
1.5 Change Drivers .....	12
1.6 DPO Appointment .....	12
2. Further Clarity on Certain Aspects of the GDPR.....	13
3. Consent & Legitimate Interest .....	14
3.1 Impact of New GDPR Consent Requirements .....	14
3.2 Legitimate Interest Processing .....	16
4. Records of Processing & Data Mapping.....	17
4.1 Data Life Cycle Tracking .....	18
4.2 Data Tagging & Classification.....	19
5. DPIA & Security Design Assessments.....	19
5.1 Data Privacy Impact Assessments.....	19
5.2 Security Design Assessments .....	22
6. Automated Decision-Making .....	23
7. Controller - Processor Relationship & Agreement.....	24
7.1 Controller – Processor Agreements .....	24
7.2 Obligations for Processors .....	25
8. International Data Transfers .....	26
9. Breach Notification .....	28
10. Main Establishment.....	29
11. Right of Data Portability.....	30
12. Seals & Certification .....	31
About the Centre for Information Policy Leadership.....	32
About AvePoint.....	33
Glossary & References.....	34

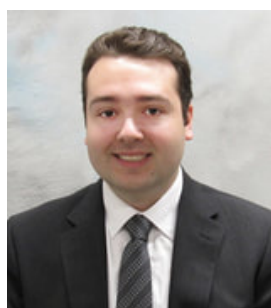
# Foreword



**Bojana Bellamy**

*President, Centre for Information Policy Leadership*

With May 2018 just around the corner, organisations have spent much of the last two years preparing for the significant impact the GDPR will bring to their data privacy compliance in Europe and globally. The GDPR will have commercial, business and legal impacts on how organisations manage and use data in the modern information age. The way organisations have responded to these changes varies widely from using GDPR to review their data management strategies, drive digital trust and confidence to building new comprehensive compliance programmes, reviewing IT, systems and processes, to new procedures for facilitating the exercise of individual rights. The second edition of the GDPR impact and readiness survey report provides key insights for organisations to understand and benchmark progress made across major areas of GDPR implementation while supporting internal change management programme efforts ahead of May 2018 and beyond.



**Samuel Grogan**

*Global Privacy Policy Analyst, Centre for Information Policy Leadership*

The GDPR represents the biggest change to the global privacy and data protection landscape in the last two decades. While many of the elements of the 1995 Directive will carry over into the GDPR era, there are quite a number of new requirements which organisations have been working diligently to comply with. Implementing appropriate procedures, systems and controls to achieve such compliance has been an ongoing task for organisations, with some more prepared than others. The second edition of the GDPR impact and readiness survey report details these efforts to date and paints a vivid picture of current compliance levels.



**Dana Simberkoff**

*Chief Risk, Privacy & Information Security Officer, AvePoint*

The EU GDPR like most other privacy and security laws, in many ways, reframes or reimagines the best practices that companies have been in part implementing for a number of years. But the time is now to put good policies, procedures AND technical controls in place. Moving forward with a GDPR strategy in combination with policies, education, technical automation and measurement will enable organisations to appropriately balance collaboration and transparency with data protection and privacy. The GDPR sets out a clear mandate for privacy, security and IT teams to work closely together along with their business stakeholders to ensure that data is created, collected, used, shared and end-of-lived appropriately. AvePoint is committed to helping our global customers achieve these goals. We hope that this benchmark report will allow organisations to accelerate their progress toward true operationalisation for GDPR readiness.

# Executive Summary



The European Union General Data Protection Regulation (GDPR) enters into force on 25 May 2018 and will change the landscape of personal data processing for the future. Companies, in anticipation of the forthcoming changes, have spent much of the last two years preparing to bring their privacy compliance programmes, data processing practices and IT systems and infrastructure in line with the requirements of the new Regulation. Preparations, both in scope and implementation, have varied among different organisations.

In May 2016, the Centre for Information Policy Leadership (CIPL) and AvePoint launched a global survey to understand organisational preparedness for GDPR implementation and create a snapshot of companies' readiness for the new law. Following publication of the findings in the first edition of this report (2016 Report),<sup>1</sup> CIPL and AvePoint launched the second global survey in 2017 to further understand GDPR readiness among organisations and to benchmark progress made since the first survey.

The updated survey focused on many of the same key change areas and topics of the 2016 report, along with some new areas, all of which relate to everyday business and compliance concerns for organisations.

The survey respondents totalled 239, with predominantly multinational organisations. Of the participating organisations, the majority operate in Europe (89%) and over half in the United States (55%). Over two fifths of organisations operate in the Asia-Pacific Region (46%), and over one third in the Indian (35%) and Latin American (38%) markets. The respondents represent organisations from over 25 different industry sectors with information technology companies (24%), business and professional services (7%) and financial services (6%) representing the highest portion of respondents. This was followed by respondents from healthcare, marketing and advertising and manufacturing sectors (all at 5%).

The 2017 survey results reveal the following key trends:

1. **GDPR Impact, Organisational Readiness & Resources:** Building and maintaining a comprehensive privacy compliance programme, rules surrounding data security and breach notification and compliance with individual rights continue to be areas of high change impact on organisations. Core processing principles are reported to present a higher change impact than in 2016 and this could be as a result of organisations working to re-engineer systems and processes to comply with the newly introduced principles ahead of 25 May 2018. Senior management continues to express concern around the enhanced sanction regime and stricter rules on consent and the reuse of data. This year, restrictions on profiling and enhanced individual rights appear to present a higher concern than they did previously. To tackle these concerns and change impacts over half of all respondents have committed additional budget to GDPR implementation with increases ranging from hundreds of thousands of dollars to upwards of \$50 million. This wide range is reflective of the fact that organisations vary in their GDPR implementation status and that there is a large spectrum between organisations that have mature privacy programmes and those that are just starting.

2. **Areas in Need of Further Clarity:** Respondents noted that legitimate interest remains the area in need of most clarity under the GDPR, followed by data protection impact assessments and risk, breach notification, notice and consent and privacy by design. These are complex topics and ensuring their correct implementation is by no means a light task. Organisations will have to work hard to find and demonstrate best practices to ensure compliance with all aspects of the GDPR, including less straightforward aspects. The EDPB and national data privacy regulators will have a continued role to play in clarifying the less certain areas.
3. **Consent and Legitimate Interest:** The GDPR introduces new requirements which organisations will have to comply with to ensure they obtain valid consent from individuals before processing their data on that basis. Organisations reported that ensuring individuals can withdraw consent at any time, ensuring consent is evidenced and documented, and ensuring consent is separate for each processing operation will most impact their current practices for obtaining consent. Almost half of the organisations reported they will increasingly rely on legitimate interest to process data once the GDPR enters into force. This is reflective of the increased difficulty in obtaining valid consent under the GDPR and also that organisations view legitimate interest as a more appropriate processing ground for many data processing contexts in the modern information age.
4. **Records of Processing and Data Mapping:** While technology tools and software are the number one priority for GDPR-focused budget spending, much work is still to be done to assess and procure these solutions. The survey data shows that respondents still rely heavily on manual methods for building and maintaining inventories of their data processing. Only a fifth of respondents use automated software tools to track their data's full life cycle and almost 60% of organisations do not have any procedures in place to identify and tag data. Of those that do, only 9% use automated tagging. This is one area where organisations will need to invest in technology and tools to build and automate these processes to ensure compliance with several GDPR requirements. The role of a DPO or privacy team as "technology buyer" will be pertinent to such investments. IT and IS stakeholders should also be part of these investment and purchasing decisions.
5. **DPIA and Security Design Assessments:** Almost 50% of organisations reported that they carry out DPIAs in circumstances envisaged by the GDPR. However, almost a quarter feel DPIAs are not applicable to their organisation. It will be crucial that organisations assess their processing operations to see whether any of their data processing activities could result in a high risk for individuals. A similar number of organisations conduct security design assessments for the creation of new IT systems or processes. For organisations that carry out DPIAs and security design assessments, the process remains mostly informal, with most relying on the use of spreadsheets or Word documents with questions. As with data classification and tagging, investing in appropriate technology will be essential to ensuring compliance for new data processing activities.
6. **Automated Decision-Making:** Over two thirds of organisations reported that they carry out some form of automated decision-making. There appears to be confusion among organisations as to which types of automated decisions fall within the scope of Article 22 of the GDPR, with many reporting profiling alone as an example of automated decisions they take under Article 22. It is important that organisations critically assess whether their automated decisions in fact produce legal or similarly significant effects, bearing in mind that this is a high bar to meet and the application of Article 22 is reserved for only truly impactful solely automated decisions.



7. **Controller-Processor Relationship and Agreement:** Over two fifths of organisations started reviewing and renegotiating their processing contracts in 2017. However, almost a quarter of organisations have not yet implemented any processes to update their contracts or review or renegotiate existing agreements. Some GDPR required terms are already included in existing contracts by some organisations but overall, organisations will have to closely look at all their controller-processor agreements ahead of 25 May 2018 to ensure they include all the new required terms introduced by the GDPR. In respect of processor obligations, maintaining records of all processing activities was reported as requiring the most internal consideration and change for organisations. This was followed by complying with the terms of the controller/processor agreement. This is not surprising given that the data shows there is much work to be done to update such agreements.
8. **International Data Transfers:** Organisations continue to use a wide variety of transfer mechanisms to legitimise data transfers outside the European Union, depending on the type and circumstances of the transfer. Model clauses remain the current most popular transfer mechanism, followed by the Privacy Shield and necessity of contract. Post-GDPR, reliance on model clauses will increase, along with reliance on the Privacy Shield and Binding Corporate Rules. Despite little information being available on new GDPR transfer mechanisms such as adequate safeguards and certifications, for the second year in a row, respondents indicated they are likely to use these mechanisms, with almost a fifth of organisations reporting they will rely on the latter post-GDPR.
9. **Breach Notification:** Given the rise of cyber-attacks in the modern information age and new security breach notification requirements under the GDPR, along with potentially massive penalties for failing to properly handle breaches, companies will have to work to ensure they have appropriate security measures and procedures in place ahead of 25 May 2018. Encouragingly, the majority of organisations have put internal reporting procedures and incident response plans in place. However, organisations still have some work to do in implementing other data breach response procedures such as conducting dry runs and retaining PR and media consultants. Almost two fifths of respondents have procured cyber insurance coverage.
10. **Main Establishment:** A significant proportion of organisations will be able to benefit from the main establishment and lead supervisory authority provisions of the GDPR. About two thirds of survey respondents reported they will have a main establishment, with just over a third reporting they will have multiple establishments in multiple EU Member States.
11. **Right of Data Portability:** There continues to be confusion around the application of the right of data portability, with 54% of organisations reporting they do not consider the right of data portability to be relevant to them, or are unsure whether it is. A higher percentage of organisations are, however, implementing procedures to enable an individual to transmit his or her data to another controller in a machine readable format (22%). This is a positive increase compared to 2016 when only 10% of respondents reported having such procedures in place.
12. **Seals and Certification:** Over 50% of organisations reported they would rely on certifications to demonstrate their compliance programme, which is a significant increase on the two fifths of organisations that reported the same in 2016. This sends a strong signal in terms of industry's readiness to embrace certifications at programme level, providing they relay benefits for them. Over one third of respondents reported they would rely on certifications for specific products and services and for data transfers.

# Survey Results and Key Findings

## 1. GDPR Impact, Organisational Readiness & Resources

### 1.1 Key Areas of Impact

Based on the 2017 results, respondents identified the following areas where the GDPR will have the highest impact on their organisation and compliance:

- |  |  |
|--|--|
| a. Accountability – Privacy Compliance Programme | c. Data Security and Breach Notification |
| b. Core Processing Principles                    | d. Individual Rights                     |

Compared to the 2016 results, building and maintaining a comprehensive privacy compliance programme remains one of the highest areas of impact on organisations seeking to comply with the GDPR. This is not surprising given that accountability is the cornerstone of the new Regulation. Implementing, maintaining and being able to demonstrate a comprehensive and effective privacy programme requires a concerted and ongoing effort and considerable resources. Interestingly, 2017 survey data also show that over a third of respondents (35% vs. 21% in 2016) feel confident that they have dealt with the initial impact of the GDPR on their privacy management programme and do not perceive this as a high area of impact. This is reassuring and demonstrates that an increasing number of organisations are well advanced in the implementation of their GDPR privacy compliance and management programmes.

Additionally, data security and breach notification continue to be ranked as top areas of impact. Many companies will have to revamp their whole approach to organisational data security both internally and externally and put in place new incident response plans and breach notification readiness procedures. The GDPR introduces specific breach notification obligations for EU controllers and processors for the first time. The concerns over heightened cybersecurity threats, the increased risk profile for organisations suffering a breach and the strict 72 hour deadline for notification to regulators are likely contributing factors to the anticipated impact of this requirement on organisations. The 72 hour notice period will be particularly significant as data in our survey show that very few organisations (9%) are using automation to tag and classify their data (See Section 4.2). This becomes troubling as notifying a DPA or individuals that their personal data has been breached involves knowing what data has been impacted, accessed or lost in the first place.

Interestingly, in a change from the 2016 survey results, respondents rated core processing principles as one of the areas where the GDPR will have the highest impact (43% in 2017 vs. 30% in 2016). This confirms the high operational impact of companies having to re-engineer their systems and processes to comply with newly heightened GDPR requirements, such as transparency, consent, legitimate interest and other legal basis for processing, privacy by design, data protection impact assessments (DPIAs), etc. As more guidance on the principles becomes available from regulators and the Article 29 Working Party (WP29), companies may have to integrate further changes into their organisations, resulting in an even higher change impact.

Finally, compliance with individual rights is one area where more organisations are reporting a higher impact than in 2016 (38% vs. 31%). This is consistent with the increased concern of senior management over compliance with individual rights (See Section 1.2 below). This is not surprising as organisations are starting to implement more robust procedures for the exercise of individual rights. There is a real expectation that more individuals will be exercising their rights under the GDPR, as the awareness and communication around the GDPR (as well as transparency requirements of the GDPR) increase.

Please rate the impact that the following new GDPR requirements will have on your organisation						
	Minimal Impact		Medium Impact		High Impact	
Compliance Area	2017	2016	2017	2016	2017	2016
Core Processing Principles	38%	42%	19%	27%	43%	30%
Individual Rights	37%	37%	24%	33%	38%	31%
Privacy Compliance Programme	35%	21%	18%	31%	47%	49%
Use and Contracting with Processors	40%	27%	27%	29%	33%	44%
New Obligations on my Organisation as Processor	43%	44%	26%	24%	32%	32%
Data Security and Breach Notification	35%	34%	23%	26%	41%	41%
International Data Transfers	49%	44%	19%	23%	32%	33%

## 1.2 Top Areas of Senior Management Concerns

Senior management concerns about GDPR readiness and implementation remained largely the same in 2017 with enhanced sanctions ranked as the leading concern (44%). Enhanced individual rights (41%) and stricter rules on consent and the ability to reuse data (39%) continue to cause high concern, while there has been an increase in concern surrounding restrictions on profiling (39%). As noted in the 2016 report, concerns surrounding rules on consent and the ability to reuse data confirm that the GDPR and data privacy compliance are closely related to a company's data strategy, big data and analytics, and that data is critical to many business processes, products and services. Profiling is one activity organisations engage in which requires reuse of data and analytics, and concern may have increased as more guidance has been released on both profiling and automated decision-making under the GDPR, particularly with respect to the direct prohibition interpretation of the latter taken by the WP29.<sup>2</sup>

Finally, concerns over the impact of security breach notification obligations have diminished, with many more organisations (40% vs. 26% in 2016) reporting that this was no longer a priority concern of senior management. This could be due to the fact that many more organisations are improving their security policies and are in the advanced stages of implementing incident response and breach notification readiness plans and procedures. However, on the other hand there are still about a third of organisations whose senior management is highly



concerned about the impact of breach reporting obligations. This is also consistent with survey results on readiness for change, discussed in Section 1.3 below.

Senior Management Concerns about the GDPR						
	Not Concerned		Medium Concern		Highly Concerned	
	2017	2016	2017	2016	2017	2016
Enhanced Sanctions Regime	35%	27%	20%	28%	44%	45%
Stricter Rules on Consent and Reuse of Data	38%	31%	23%	35%	39%	34%
Restrictions on Profiling	44%	37%	18%	35%	39%	28%
Enhanced Individual Rights	34%	32%	25%	35%	41%	33%
International Data Transfers	44%	39%	20%	29%	35%	32%
Additional Processor Obligations	36%	37%	28%	32%	36%	30%
Data Security Breach Reporting	40%	26%	29%	36%	32%	38%
Changes to Internal Privacy Compliance Programme	37%	33%	26%	34%	36%	33%

### 1.3 Readiness for Change

In 2016, less than one third of respondents reported feeling fully or nearly compliant with key aspects of the GDPR. An equal number of respondents felt the same way in 2017. However, there has been a change in the type of compliance areas of the GDPR that organisations report feeling least ready for.

Organisations appear to be least ready in respect of:

- a. International Data Transfers
- b. Core Processing Principles
- c. Data Security and Breach Notification / New Obligations on my Organisation as Processor

In 2016, only 35% of respondents reported being nearly or fully compliant with implementing GDPR requirements on international data transfers. The 2016 report noted that this may reflect mounting legal uncertainty around existing transfer mechanisms and the fact that organisations will have to consider new mechanisms to justify different types of transfers under the GDPR. This trend has largely continued, with an even lower percentage of respondents in 2017 reporting they are nearly or fully compliant with data transfer requirements (27%). Over half of the respondents reported that they did not feel their organisation was ready in respect of international data transfers requirements compared to one third in 2016. This shows that data transfers remain an important and challenging area of legal compliance for most organisations. The drop in confidence is likely due to continued uncertainty regarding existing data transfer mechanisms. These include: forthcoming legal challenges to standard contractual clauses in the Court of Justice of the European

Union (CJEU); the administrative burdens of BCR approvals and a lack of clarity on how to update the BCR to be in line with the GDPR; the uncertainty and geographic limitations of the Privacy Shield (covering only transfers to the United States) and, at the time of the survey, the pending results of the Shield's first annual review; the lack of clarity around the application of derogations and certifications as a new transfer mechanism under the GDPR; and finally, the impact of Brexit on data flows. This is consistent with the survey findings on areas of the GDPR requiring further clarity (See Section 2) — with between a quarter to a third of respondents citing international data transfers, Privacy Shield and Brexit as requiring further clarification.

Newly introduced requirements surrounding core processing principles and obligations for processors continue to be areas where organisations feel least ready (49% and 44% respectively). Respondents reported feeling even less ready for data security and breach notification in 2017 compared to reported rates for 2016 (44% vs. 33% in 2016).

Interestingly, a higher number of respondents felt nearly or fully compliant with the requirement of accountability and implementing a privacy compliance programme (which corresponds to the findings on areas of impact in Section 1.1 above). Given that many respondents rated this requirement as having the highest impact on their organisation two years in a row, we suspect many organisations have dedicated a great deal of resources and a lot of effort to implementing a comprehensive privacy management programme and with these efforts comes an increase in confidence in GDPR readiness.

Please indicate how ready you consider your organisation to be for the following under the GDPR						
	Neutral		Process Underway		Fully Compliant	
	2017	2016	2017	2016	2017	2016
Core Processing Principles	49%	35%	26%	36%	26%	30%
Individual Rights	43%	47%	31%	29%	26%	24%
Privacy Compliance Programme	39%	43%	31%	35%	30%	22%
Use and Contracting with Processors	42%	37%	31%	39%	27%	24%
New Obligations on my Organisation as Processor	44%	43%	32%	35%	24%	22%
Data Security and Breach Notification	44%	33%	25%	30%	31%	37%
International Data Transfers	52%	33%	21%	32%	27%	35%

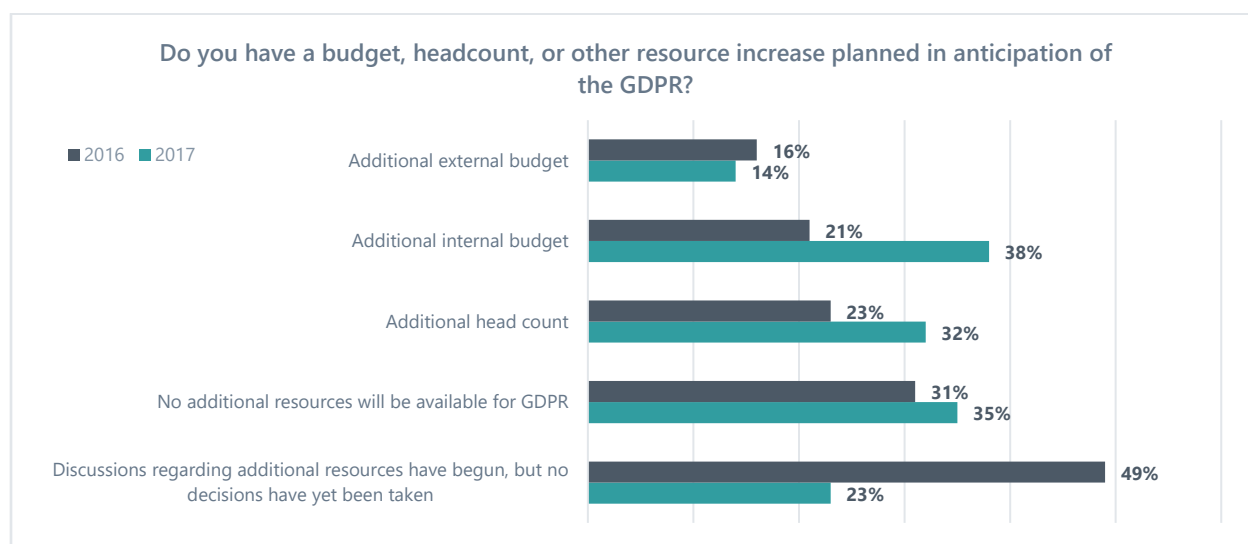
## 1.4 Impact on Resources

At the close of the 2016 survey, less than one fifth of organisations had actually committed additional headcount, budget or external counsel spend for GDPR implementation and almost one half of respondents were still in discussions regarding resources but had not taken any action.

Less than one year later, the results show that this trend has largely flipped with over half of respondents (52%) reporting they had committed additional budget and just over one fifth of organisations still undergoing internal discussions about resources (23%). Additionally, one third of organisations (32%) reported they have committed additional headcount for GDPR implementation vs. just under a quarter (23%) in the 2016 survey.

Budget increases for GDPR implementation range from hundreds of thousands of dollars for some organisations to upwards of 50 million dollars for others. This wide range is reflective of the fact that organisations vary in their GDPR implementation status. A large spectrum exists between those with mature privacy programmes and those that are just starting, as well as between those that may be more impacted by the GDPR based on their business model and the instances of processing of personal data. Technology solutions and services ranked as the highest priority for organisations in distributing their additional GDPR budget. This is consistent with the trend we have noted in the 2017 survey as opposed to the 2016 results — with an increasing number of organisations looking for tools and technologies to operationalise and industrialise their GDPR compliance and an increased offering of such tools and technologies in the marketplace. The budget for such solutions and services may be well spent, as the survey results will show, in areas such as tagging, classification, automating DPIAs and data mapping and records of processing. There will be a major shift in organisations in the role of a DPO or privacy team as “technology buyer”, as this has not previously been a standard function for this role. This too will require a multi-disciplinary team to ensure that IT and IS team members are stakeholders in these purchasing decisions. External advisory support ranked as the second highest priority for organisations which secured a one-time GDPR budget increase, while additional staff and training for staff represented the second highest priority for organisations which secured an ongoing budget increase.

Similar to last year, just over one third of organisations (35%) reported they will not have additional resources made available to them for GDPR compliance. Though this figure is concerning, given that the GDPR was less 9 months away at the time of the survey, one could interpret this to mean that these organisations already had existing adequate resources or that their privacy programme is mature enough not to warrant a complete overhaul.



## 1.5 Change Drivers

The GDPR requires organisations to implement a plethora of changes to the way they manage their data, IT systems and internal and external business processes. The changes vary across the organisation from new processes for transparency and legal bases of processing, to contracts between controllers and processors, to new data privacy impact assessment processes, to security policies and procedures and frameworks for international data transfers. Given the volume and complexity of change required, organisations have realised that GDPR implementation requires a change management programme. About a third of organisations have set up cross-departmental steering committees to drive GDPR implementation.

Legal departments still ranked as the highest drivers of change in anticipation of the GDPR (58%). This was followed by IT and compliance departments (42% and 41%, respectively) and information security departments (32%). 15% of respondents reported other departments were driving GDPR implementation. Among them data protection officers (DPOs) were most frequently cited.

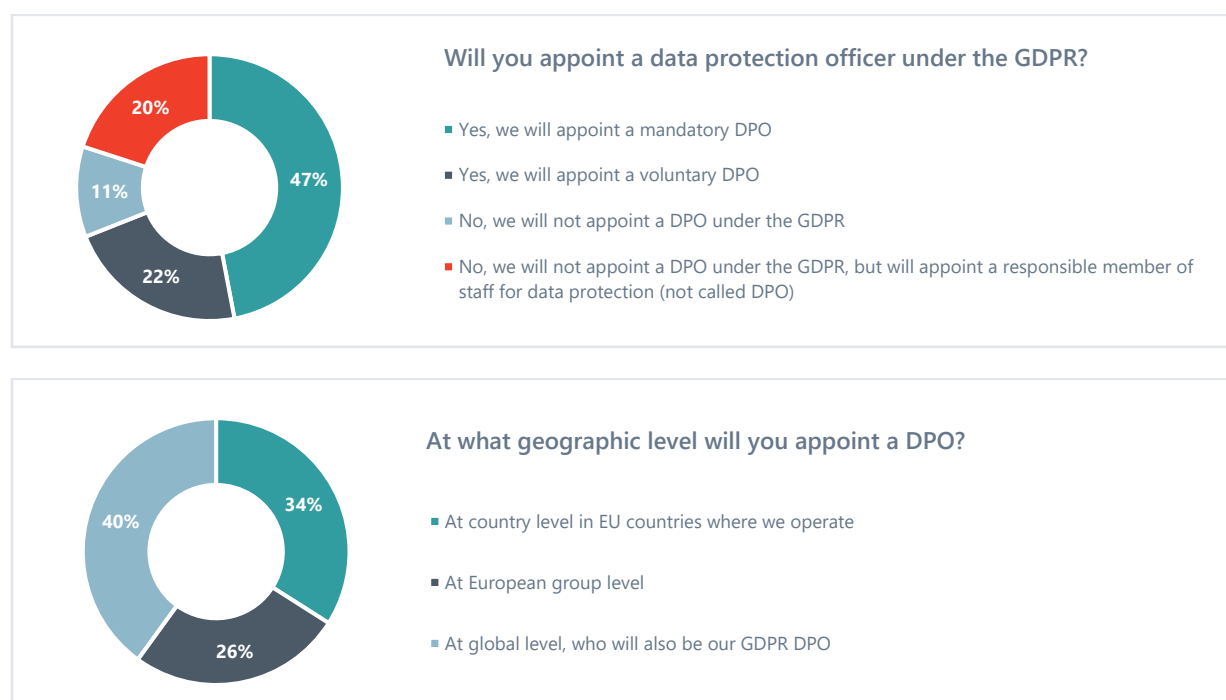
Which departments are driving GDPR implementation within your organisation?	
Legal	58%
Compliance	41%
IT	42%
Information Security	32%
Cross-Department Steering Committee	32%
Other	15%

## 1.6 DPO Appointment

Given the increased focus on accountability under the GDPR and the need for organisations to ensure ongoing compliance after 25 May 2018, it is not surprising that the majority of survey respondents (89%) will either appoint a statutory DPO under the GDPR or a responsible member of staff with similar duties. Almost half of all survey respondents report that they will appoint a mandatory DPO under the GDPR (47%) with a further 22% reporting that they will appoint a voluntary DPO. The latter represents cases where organisations are not legally required to appoint a DPO under Article 37 of the GDPR, but they nevertheless decide to appoint a voluntary DPO with the same statutory responsibilities as a mandatory DPO.

Finally, 20% of respondents reported that although they will not formally appoint a DPO under the GDPR, they will appoint a responsible member of staff for data protection to drive GDPR compliance. It is encouraging to see that although certain organisations may not be required to appoint a formal DPO as per GDPR criteria, they still recognise the importance of ensuring ongoing responsibility for data protection through a responsible member of staff. Only 11% of respondents report that they will not appoint a DPO, a slight decrease from the 2016 survey where 15% had not appointed a DPO. This signifies that the role of the DPO is becoming more crucial to all types of organisations seeking to implement the new requirements of the GDPR and ensure compliance on an ongoing basis.

The survey also sought to understand if multinational organisations are appointing DPOs at EU, country or global level. Regarding the geographic level of appointment, 40% of respondents reported they will appoint a DPO at global level, who will also serve as the organisation's GDPR DPO. Just over a third of respondents will appoint a DPO at country level in EU countries where they operate and just over a quarter of organisations will appoint a DPO at European group level. It's interesting to see that organisations are taking different approaches to DPO appointment at the geographic level and confirms that some flexibility is needed for organisations in how they implement the DPO requirement under the GDPR.



## 2. Further Clarity on Certain Aspects of the GDPR

As noted in the 2016 report, even though some of the GDPR concepts are the same as in Directive 95/46/EC (the Directive), their implementation, interpretation and circumstances in which they apply will change. Since the first survey concluded, a great deal of GDPR guidance has been released by national data protection authorities (DPAs) and the WP29. Nevertheless, many open issues remain, hence the 2017 survey asked respondents about aspects of the GDPR that require further clarity for their organisations.

Among the 124 organisations that answered this question, legitimate interest remains the area in need of most clarity (47%).

Despite guidance being released between the initial report and this survey on data protection impact assessments and risk, 44% of respondents seek further clarity on PIA and Risk. Breach notification, notice and consent and privacy by design were the next most popular areas in need of further clarity. Since the



survey concluded, WP29 guidance on breach notification has been finalised<sup>3</sup> and proposed guidelines on consent have been released<sup>4</sup> which may provide further insights for companies.



### 3. Consent & Legitimate Interest

The standard of consent, as a lawful ground for personal data processing, is higher under the GDPR than under the Directive. The GDPR introduces new requirements which organisations will have to comply with to ensure that they obtain valid consent before processing data on this basis.

#### 3.1 Impact of New GDPR Consent Requirements

In the 2016 survey, only one third of organisations reported that they were fully able to comply with the enhanced consent requirements of the GDPR. To understand further which of the new requirements of consent will impact organisations the most, the 2017 survey included a question asking companies to rate the impact each new requirement will have on its current practices for obtaining consent.

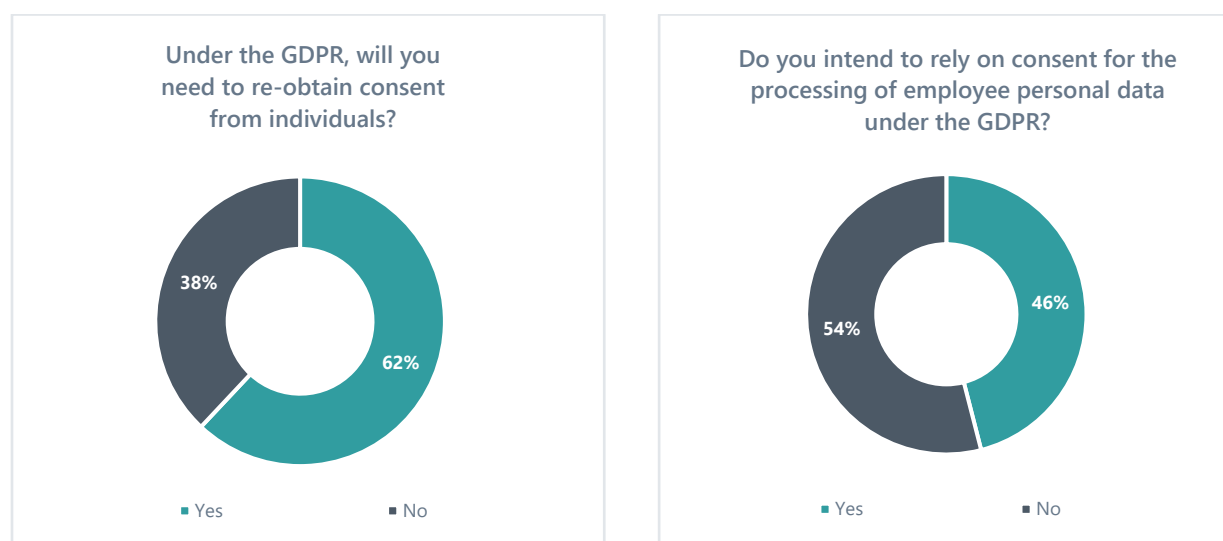
Respondents reported “ensuring individuals can withdraw their consent at any time” as having the most significant impact. This is not surprising given that many organisations find it difficult to obtain and record consent in the first instance let alone reverse it and honour the withdrawal of consent across all their systems. The second and third most impactful consent requirements rated by respondents were “ensuring consent is evidenced and documented, including the withdrawal of consent” and “ensuring consent is separate for each processing operation”.

“Obtaining parental consent or authorisation when processing personal data relating to children” and “ensuring consent is not conditional on the performance of a contract” were ranked as having the least impact on current practices. The former may be attributed to the fact that not all of the organisations are engaged in the provision of information society services offered directly to children. On the other hand well over a quarter of organisations (28%) noted that the new requirement of obtaining parental consent for children under the digital age of consent (13-16) would have a high impact for their organisation. Interestingly, in 2016, 25% of organisations reported that they require individuals to consent to the processing of personal data as a condition of using a product/service and 50% reported that they sometimes require this. The decrease in the impact of this requirement may be indicative of organisations being well under-way in refreshing their consent processes, websites, terms and conditions, privacy policies and other consent mechanisms in anticipation of the GDPR, so that consent is not conditional to the provision of products or services.

Please rate the impact the following new GDPR consent requirements will have on your organisation's current practices for obtaining consent?			
New Consent Requirement	Minimal Impact	Medium Impact	High Impact
Ensuring consent is distinguishable from other terms and conditions and obtained separate from agreement on other matters	41%	23%	36%
Ensuring consent is separate for each processing operation	41%	21%	38%
Ensuring consent is not conditional on the performance of a contract	42%	24%	34%
Ensuring consent is provided by a positive action or statement of the data subject	40%	25%	35%
Ensuring individuals can withdraw their consent at any time	36%	18%	46%
Ensuring consent is evidenced and documented, including the withdrawal of consent	36%	22%	42%
Obtaining parental consent or authorisation when processing personal data relating to children	55%	17%	28%

As a result of the newly introduced requirements, many organisations may feel that their existing consents will not satisfy the higher bar of consent under the GDPR and will need to re-obtain consent from individuals. 62% of the survey respondents reported needing to do so. Additionally, given the restrictions on using consent in situations where there is an imbalance of power, such as in employment contexts, 54% of respondents reported

that they do not intend to rely on consent for processing employee data under the GDPR. However, 46% feel they will still be able to use consent in respect of employee data processing.



### 3.2 Legitimate Interest Processing

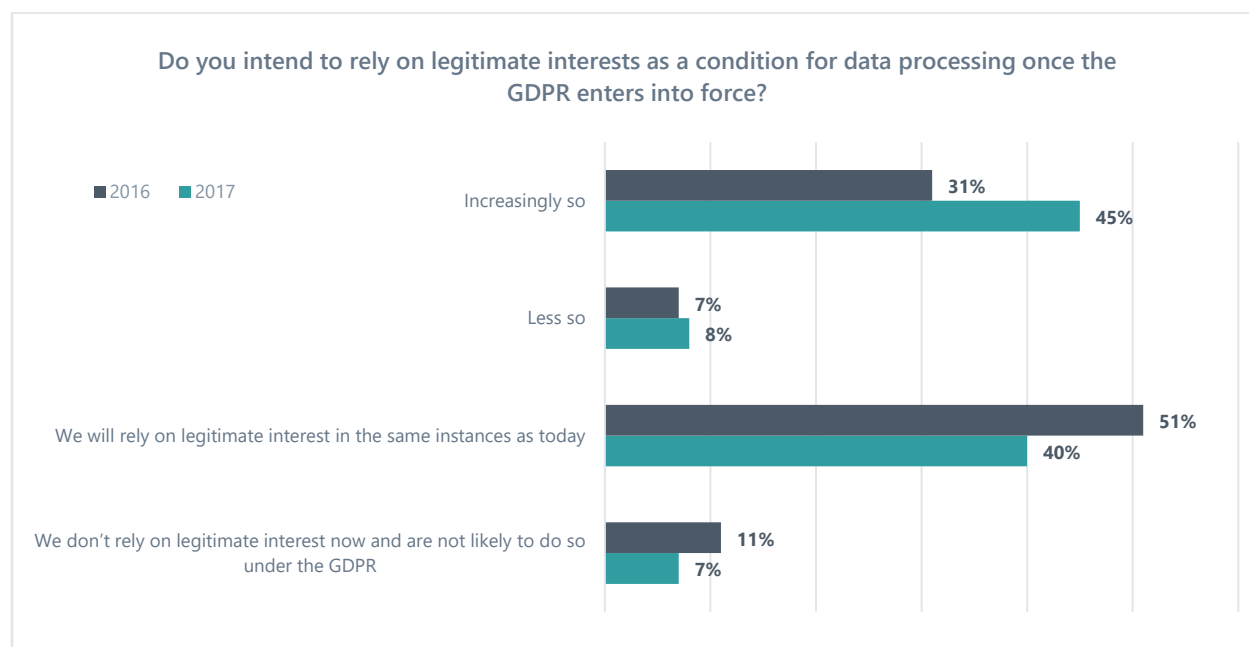
In the modern information age, there may be many contexts and circumstances in which obtaining valid consent for certain processing operations may have become impractical, impossible, ineffective or simply not meaningful: for example, where there is no direct interaction with individuals or individuals do not have a relationship with the organisation that may process their data (e.g. in the context of machine learning), where large and repeated volumes of data are processed (seeking consent at every instance may not be feasible) or where the use of data is common, expected or trivial, or privacy risk to the individual is limited.

Additionally, the practical implementation of consent can unduly burden individuals and lead to consent fatigue in certain contexts — i.e. there may be many instances where individuals simply will no longer be willing or able to keep providing consents in the face of a deluge of requests for consent from data users in the digital economy, even where they might not have an objection to the processing.

Given these complexities of using consent under the GDPR and as more organisations implement and refine comprehensive privacy management programmes, with an emphasis on accountability, it is not surprising that companies view legitimate interest as a more appropriate ground for processing for many contexts in the digital era. In the 2016 survey, 31% of respondents reported that they will increasingly rely on legitimate interest to process data once the GDPR enters into force. In the 2017 survey, this figure increased to 45%.

As noted in the 2016 report, under legitimate interest processing, organisations will still have to be accountable and undertake the full process of assessing the legitimate interest, balancing that with the rights and freedoms of individuals and implementing mitigations to reduce the impact and risks for individuals. Organisations will have to provide notice to individuals of processing based on legitimate interests, what these interests are and, furthermore, how they do not override the interests of the individuals. An additional safeguard for individuals is the reversal of the burden of proof and the right to object —

where an individual objects to processing based on legitimate interest, the burden of proof is on the controller to show that it has legitimate reasons for processing the personal data.



## 4. Records of Processing & Data Mapping

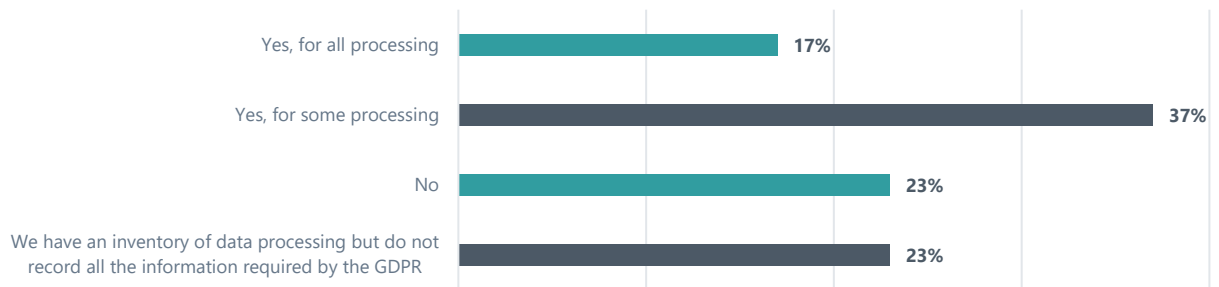
As noted in the 2016 report, the GDPR replaces the current obligation within the Directive to register processing activities and systems with DPAs with the requirement to keep internal records of all data processing activities. The new requirement applies to both controllers and processors.

54% of organisations report that they hold an up to date inventory of the personal data they hold and the purposes for which the data is processed for some or all of their processing activities. However, 23% of organisations report that they have an inventory but do not record all the information required by the GDPR. A further 23% report that they hold no inventory. Similar to 2016, it appears that there is still work to be done by organisations that will have to step up their implementation efforts and seek tools and software to assist them in complying with the data recording requirements of the GDPR.

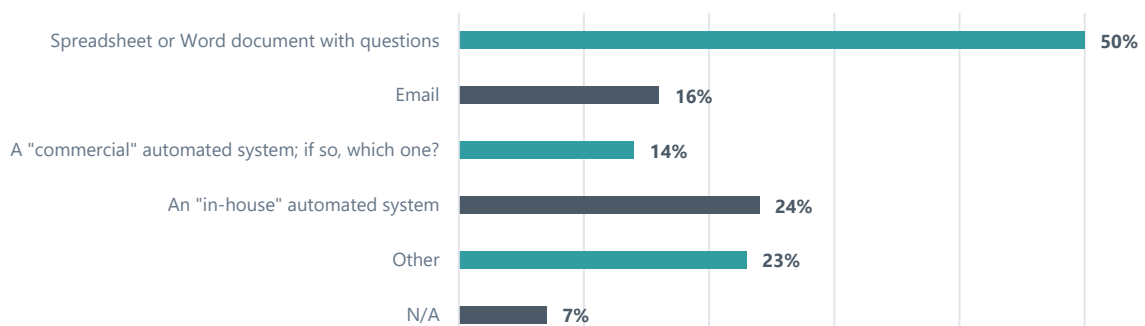
Among organisations that do maintain an inventory, half maintain this in a Word document or spreadsheet. About a quarter report using an "in-house" automated system and 14% report using a "commercial automated" system.

With respect to data transfers, almost 70% of respondents report holding a record/inventory of such information (either all the information or some of it), similar to 2016.

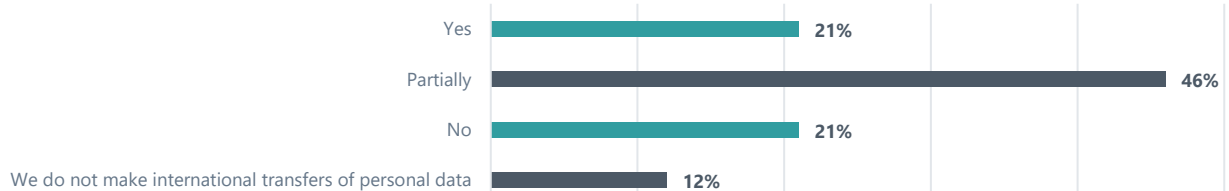
Do you hold an up to date record/register/inventory of the personal data you hold and the purpose for which they are used and other information required by GDPR?



If you maintain a record/register/inventory, which method(s) do you use?



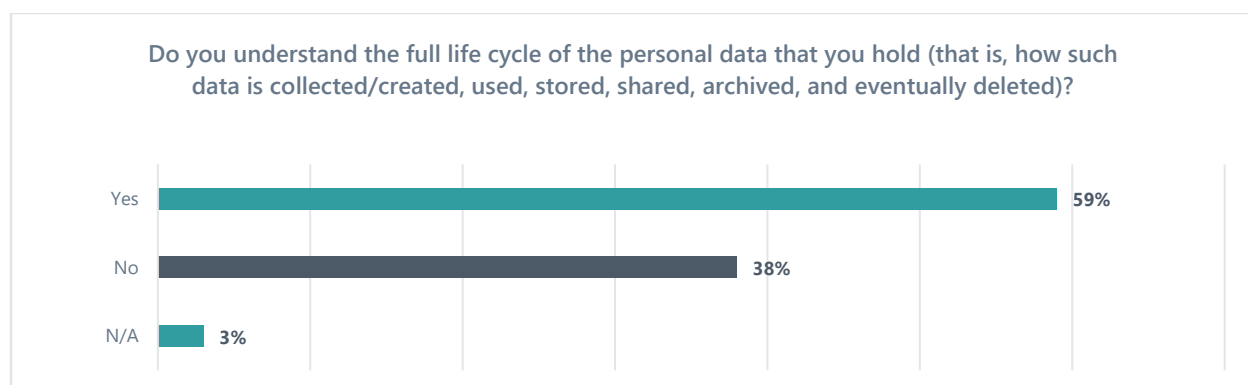
Do you hold a record/inventory of the international transfer of personal data made by your organisation?



#### 4.1 Data Life Cycle Tracking

Despite 38% of organisations reporting they do not understand the full life cycle of the personal data they hold, only 23% of respondents report using automated software tools to track their data's full life cycle. This represents an opportunity for extending a GDPR programme and building a repeatable process through the implementation of automated solutions. It also presents another opportunity to connect privacy with IT and information security — all key stakeholders in the implementation and management of this kind of system and also key beneficiaries of its effective deployment.

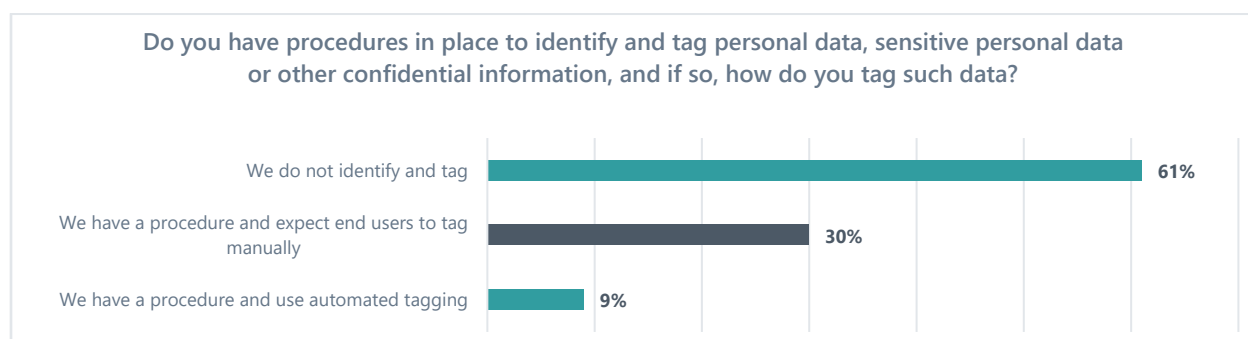




## 4.2 Data Tagging & Classification

The 2017 survey reveals that 39% of organisations have procedures in place to identify and tag personal data, sensitive data or other confidential information. This is a slight increase from 2016, when only 33% of organisations had such procedures in place. In 2017, only 9% of organisations reported using automated tagging. The other 30% have a procedure in place but expect end users to tag manually. Almost 60% of organisations still do not tag their data.

Companies will need to invest in technology and tools to build these processes and automate such tagging. End-user tagging is not sustainable or realistic in the modern data economy and furthermore, automated tagging will help organisations comply with other GDPR requirements — e.g. finding personal data for compliance with access rights, or data portability, or determining what data the organisation holds, including for breach response purposes.



## 5. DPIA & Security Design Assessments

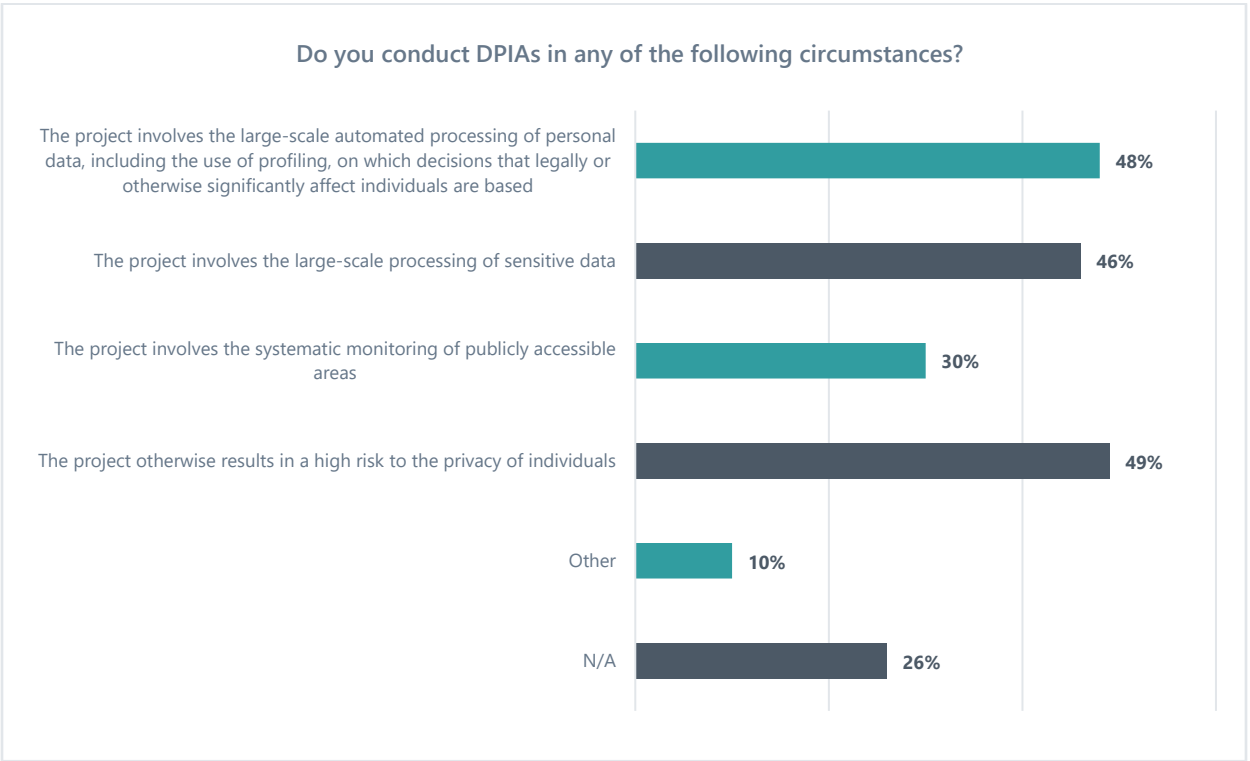
### 5.1 Data Privacy Impact Assessments

The GDPR introduces, for the first time, a requirement to conduct formal DPIAs for high risk processing. High risk processing is not defined by the GDPR but Article 35(3) states that a DPIA shall be required in the case of (i) automated decision-making producing legal or similarly significant effects; (ii) the large-scale

processing of special categories of personal data; and (iii) the systematic and large-scale monitoring of publicly accessible areas.

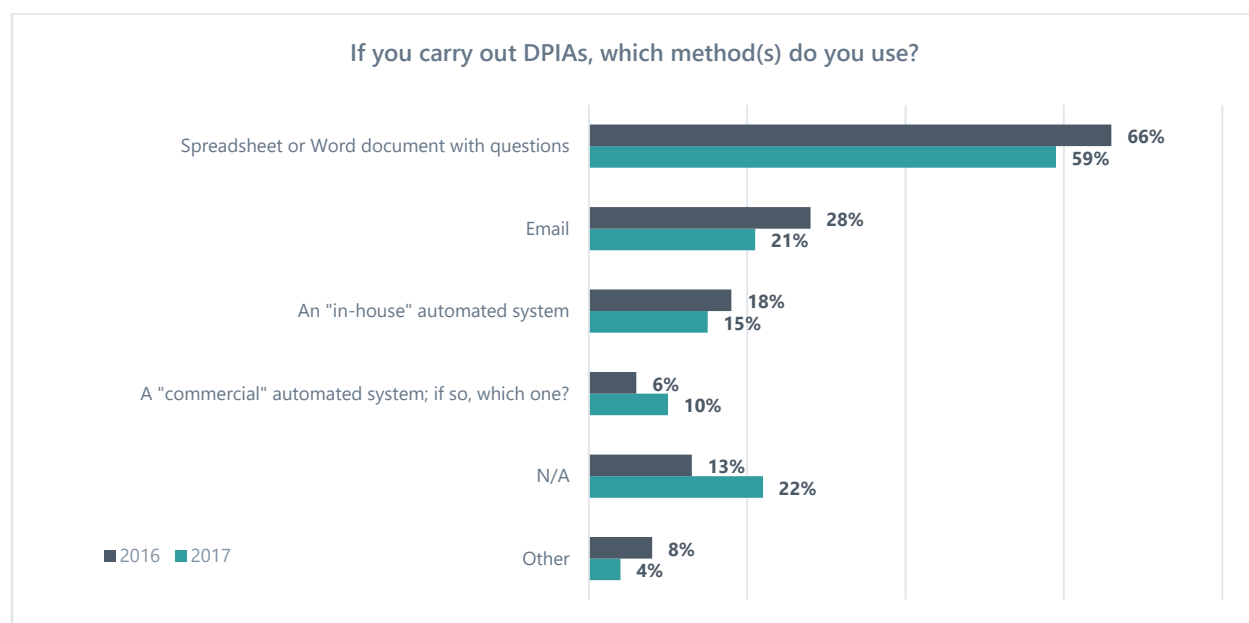
After the 2016 survey concluded, the WP29 released its DPIA guidelines.<sup>5</sup> The guidelines provide nine criteria to assist in determining whether a processing operation is likely to result in a high risk. These criteria expand the scope of where a DPIA is potentially required. As a result of these new criteria, organisations may have realised they do not currently carry out DPIAs in circumstances where the guidelines suggest they should be.

Encouragingly, almost half of all respondents reported carrying out DPIAs in circumstances envisaged by the GDPR (46%-49%). 10% of respondents report carrying out DPIAs in other circumstances, with some of them referencing the scenarios laid down in the WP29 guidelines. Nevertheless, just over a quarter (26%) of respondents reported that DPIAs are not applicable to their organisation. This may be because they do not engage in processing which is likely to result in a high risk to individuals or they are not aware that the processing activities they conduct in fact warrant a DPIA.

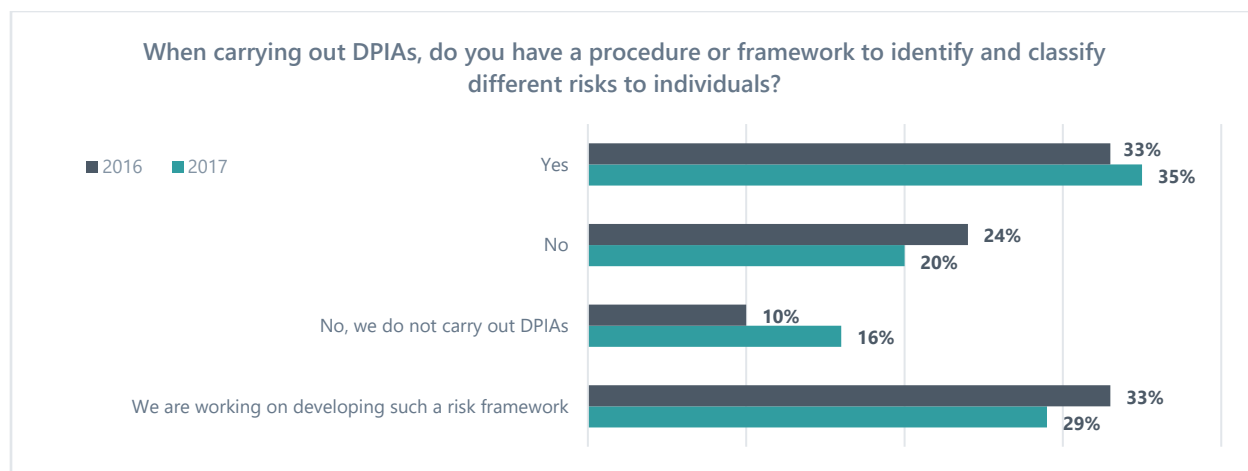


As noted in the 2016 report, the actual DPIA process is more informal for many organisations with 66% of organisations carrying out DPIAs by way of a spreadsheet or Word document with questions and 28% via email. This figure dropped slightly in 2017 (59% for spreadsheets and Word and 21% for email). This drop may reflect a shift to using more sophisticated systems to carry out DPIAs. Indeed, while only 6% of respondents reported using a commercial automated system for carrying out DPIAs in 2016, this figure rose

to 10% in 2017. Usage rates of “automated” in house systems have remained largely the same though they dropped slightly in 2017 (18% vs. 15%). Given the numerous other requirements and changes companies are working on implementing, it appears that organisations view commercial tools and software for meeting GDPR compliance as more convenient and cost-effective than building their own systems from scratch. This investment in technology will be critical for organisations to scale and industrialise their privacy programmes and compliance and effectively create repeatable processes.



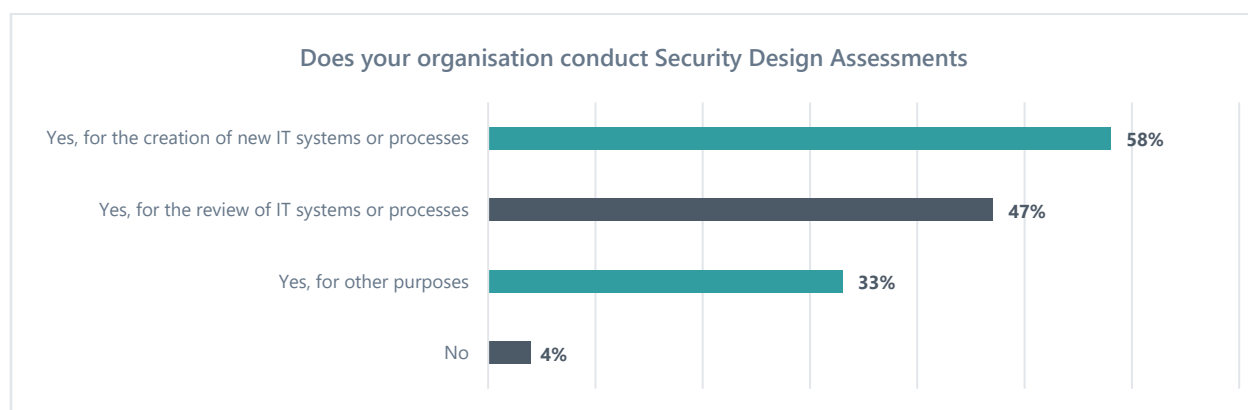
Formal risk assessment methodology within DPIAs remains largely the same — in 2016 just one third of organisations reported having a procedure or framework to identify and classify different risks to individuals and this increased slightly to 35% in 2017. The number of organisations working on developing such a risk framework has dropped, as more organisations seem to have completed this task (33% in 2016 vs. 29% in 2017). While it is not surprising that this is a complex area of implementation, there is more work to be done across a majority of organisations. As noted in the 2016 report, it will be essential that organisations develop consistent methodologies and frameworks for risk assessments, both when conducting DPIAs and in other circumstances envisaged explicitly or implicitly by the GDPR. The risk based approach to data protection is, in many ways, the underpinning of the GDPR, so the ability of organisations to demonstrate their methodology in making risk calculations through appropriate frameworks is a key factor in evidencing a true accountability and compliance programme.

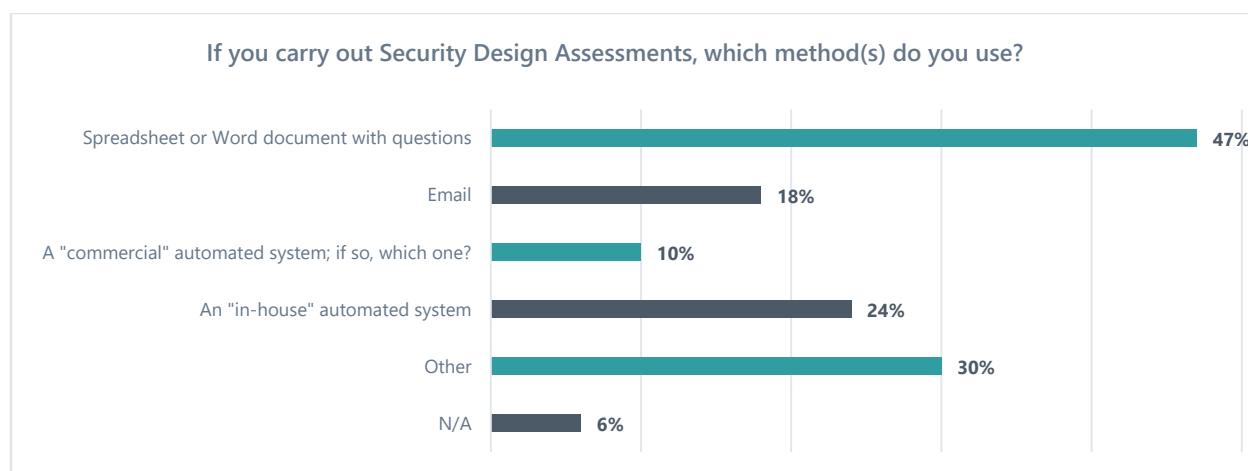


## 5.2 Security Design Assessments

Ensuring the security of data is an integral function of the Regulation and is also part of the data protection by design requirement. Compared to 2016, 18% more organisations incorporate security design assessments for new systems and processes (40% in 2016 vs. 58% in 2017) and 5% more organisations incorporate them in terms of system and process review (42% in 2016 vs. 47% in 2017). 33% of organisations report carrying out security design assessments for other purposes and encouragingly only 4% report that they do not carry out such assessments.

In terms of methods for carrying out security design assessments, 47% of organisations rely on a spreadsheet or Word document with questions, 24% on an “in-house” automated system and 10% on “commercial” automated systems. Once again, this lack of automation and reliance on spreadsheets may create an opportunity for privacy teams to join forces with their IS and CISO counterparts. Indeed, automation for security and privacy by design assessments can likely be joined, resulting in the increased spending power and utility of “GDPR” focused technologies to other key areas of the business.





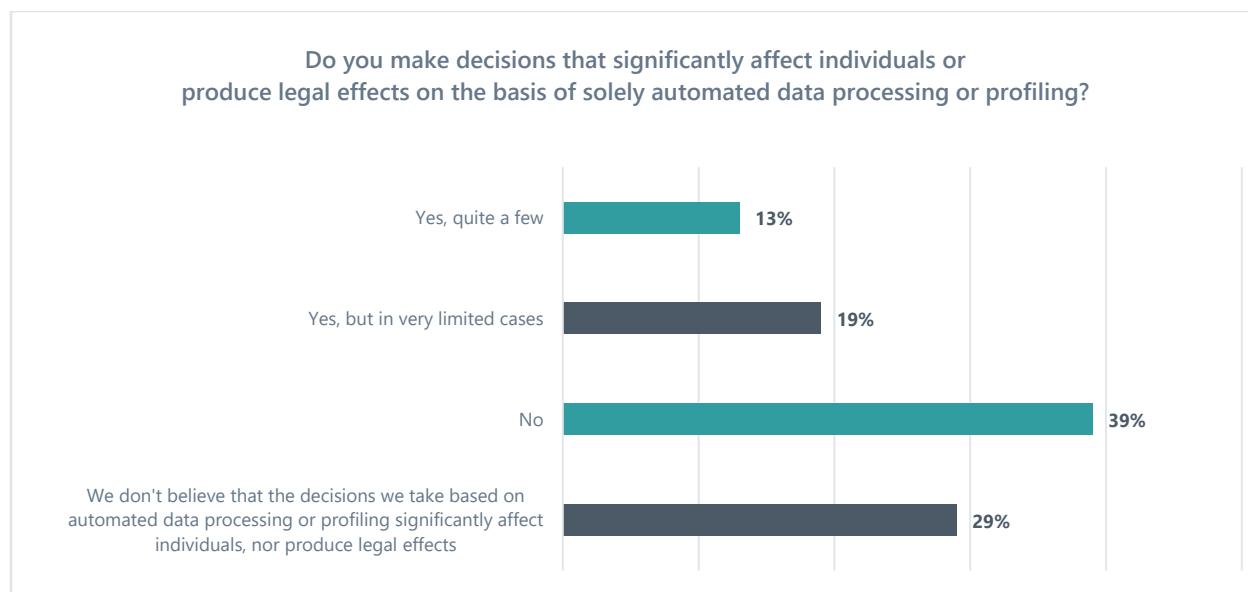
## 6. Automated Decision-Making

Article 22 of the GDPR provides that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Automated decisions have become essential to business and public sector operations in the modern digital information society. Their use will only increase with the fourth industrial revolution, the rise of artificial intelligence (AI) and machine learning and the overall increase in computing power. Hence, the survey asked respondents to indicate if they conduct automated decision-making.

The majority of respondents (61%) reported making automated decisions with only 13% reporting these automated decisions produce legal or similarly significant effects and a further 19% saying their automated decisions produce such effects in very limited cases.

Organisations were further asked to provide examples of their automated decision-making. Traditional responses such as credit worthiness assessments for loans and decisions in recruitment processes were listed. Other responses included job or customer profiling and targeted advertising. The latter suggests there is some confusion in the industry as to what constitutes an automated decision under Article 22 of the GDPR. Customer profiling alone does not comprise a decision producing legal or similarly significant effects on an individual and it is unlikely that targeted advertising constitutes such a decision either in most cases. The WP29 guidelines on individual automated decision-making and profiling even note that in many typical cases targeted advertising does not have a significant effect on individuals. It is important that Article 22 of the GDPR is interpreted narrowly to ensure that only decisions producing legal or similarly significant effects fall under the definition of Article 22, as the data shows that over two thirds of organisations are currently engaged in some form of automated decision-making.



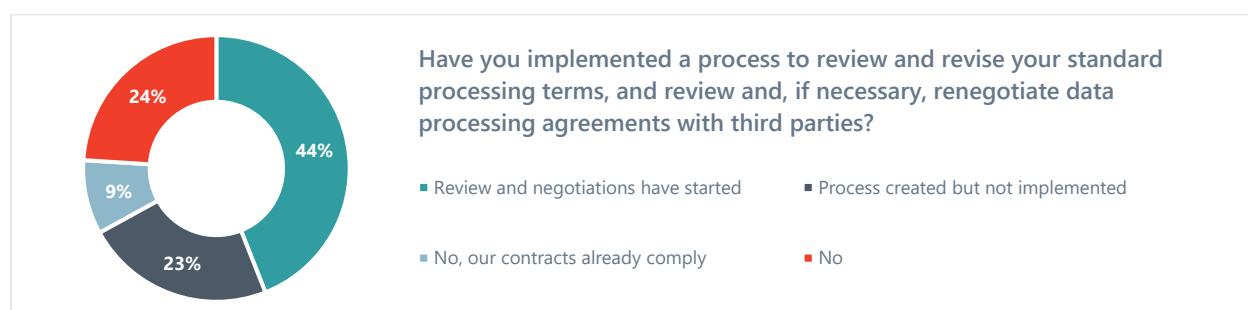


## 7. Controller - Processor Relationship & Agreement

As noted in the 2016 report, the GDPR imposes direct legal obligations on processors for the first time. The list of compulsory provisions to be included in data processing agreements between controllers and processors has also been expanded by virtue of Article 28 GDPR.

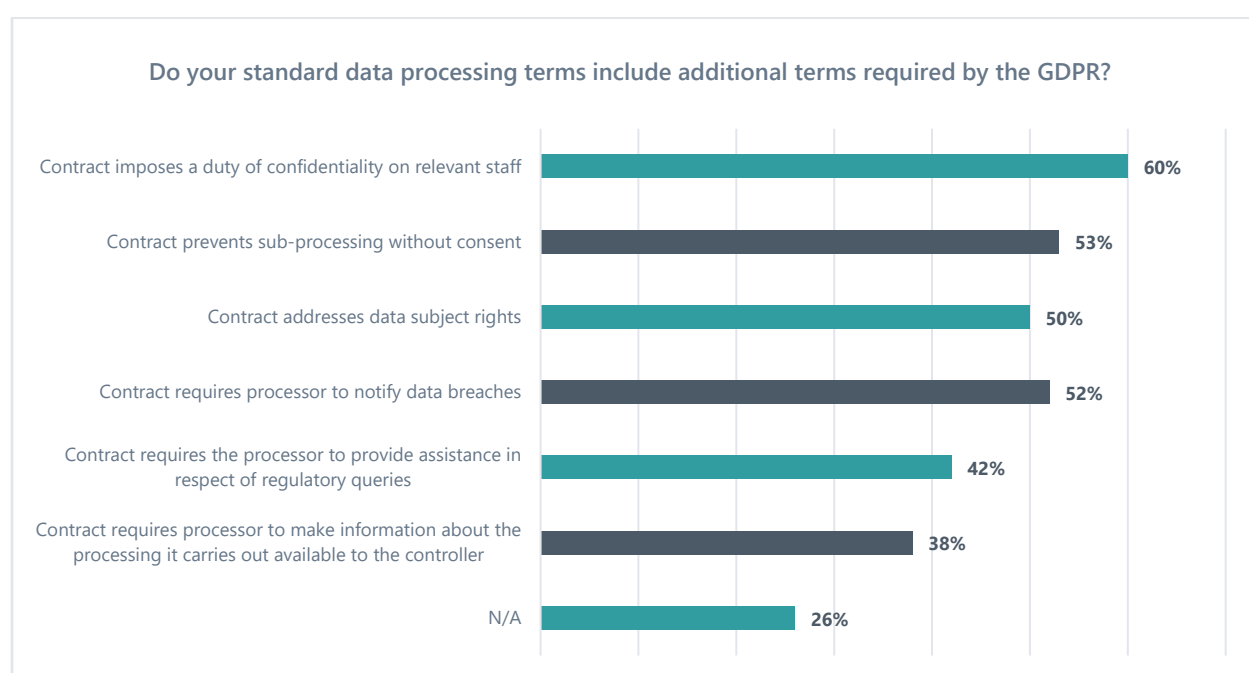
### 7.1 Controller – Processor Agreements

There has been a 12% increase in reviews and negotiations regarding processor contracts in 2017 compared to 2016 (32% in 2016 vs. 44% in 2017). Likely organisations that created but had not yet implemented their process of updating their third party contracts in 2016 have moved forward and started the review process. 9% of respondents report that their contracts already comply with the increased GDPR requirements. However, almost quarter of respondents appear neither to have implemented any processes nor reviewed or renegotiated processing agreements. This demonstrates the magnitude of the task ahead, of having to review, renegotiate and implement changes in existing and new contracts with third parties to reflect the changes in relationship and obligations between controllers and processors.



Several respondents report that they already include in their processing contracts some of the additional terms required by the GDPR (between 38% and 60%). Some terms required by the GDPR are more present than others, such as the duty of confidentiality on relevant staff and restrictions on sub-processing without consent. Other requirements, such as the obligation that a processor makes information about the processing it carries out available to the controller, are less present.

While it's encouraging that many organisations seem to already include GDPR required terms in their processing contracts, likely many organisations are still reviewing and updating their third party contract terms to be in compliance with the Regulation. The review and potential renegotiation of third party contracts is clearly a lengthy and complex process. With 25 May 2018 approaching, many organisations will have much work to do to ensure their contracts are up to standard with the GDPR both for existing contracts and for new contracts going forward.

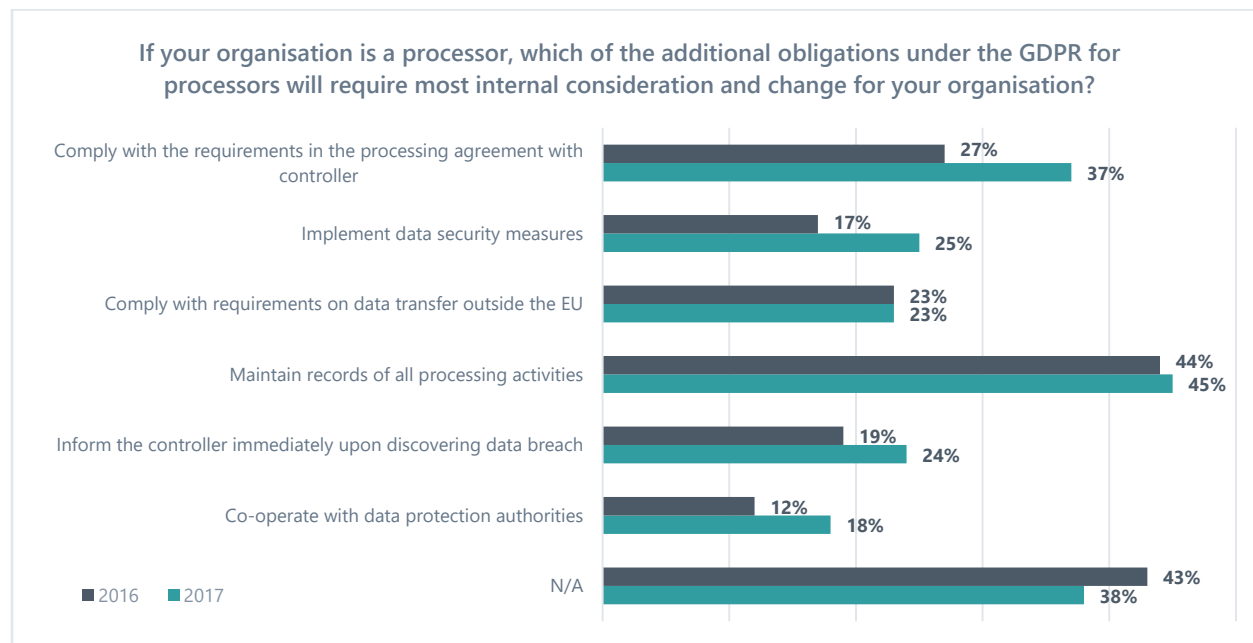


## 7.2 Obligations for Processors

In the 2016 survey, processor organisations indicated they would be most impacted by GDPR processor obligations in respect of documenting all data processing activities (43%), complying with the terms of the controller/processor agreement (27%) and data transfers outside the EU (23%).

In the 2017 survey, the concerns remained largely the same, although a larger number of processor organisations seem to be aware of the increased impact of the new obligations. Maintaining records of all processing activities was reported as requiring the most internal consideration and change for organisations (45%). This is not surprising as it is likely that many processors have been in a position to review and renegotiate changed terms of processing agreements, and therefore consider the impact of the enhanced

requirements. Complying with the terms of the controller/processor agreement remains the second most impactful obligation on organisations (37%). Implementing data security measures was reported to be the third most impactful processor obligation on organisations, increasing upon last year's reported figure (17% in 2016 vs. 25% in 2017).



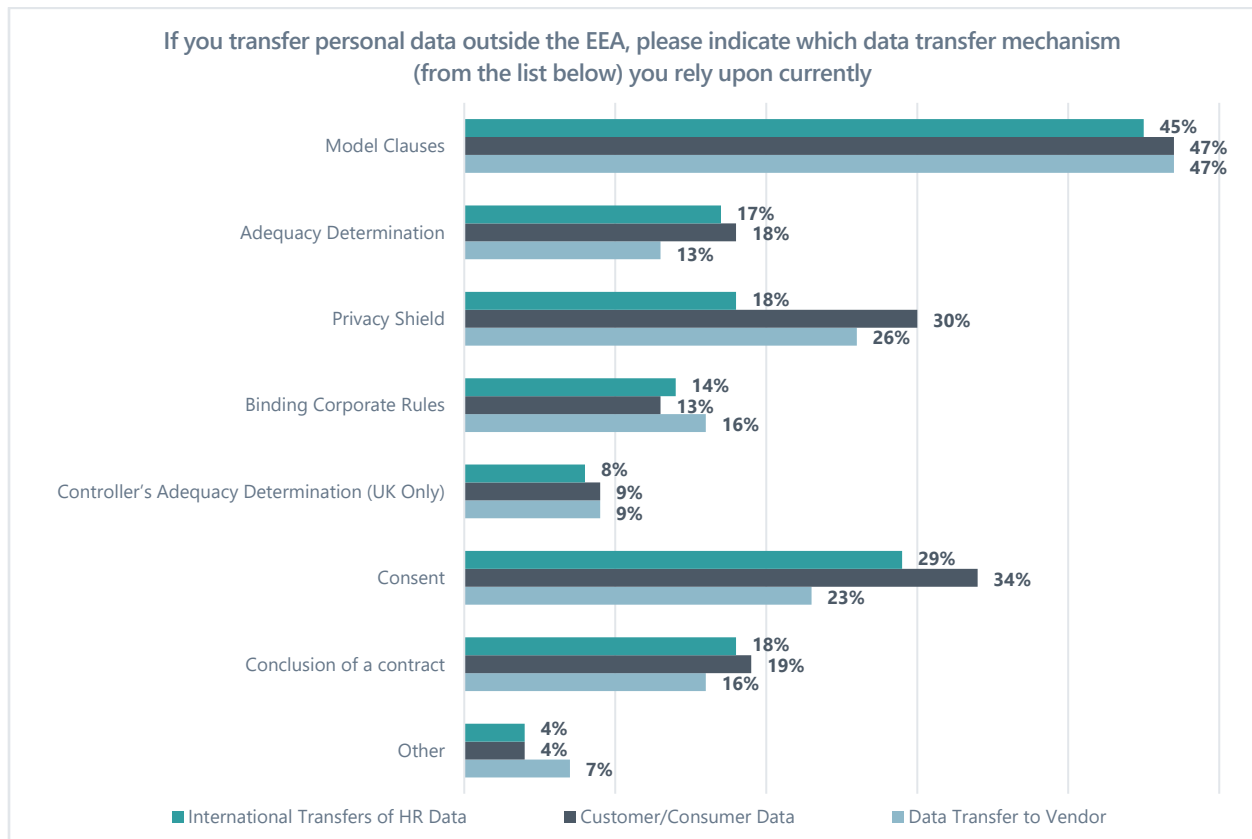
## 8. International Data Transfers

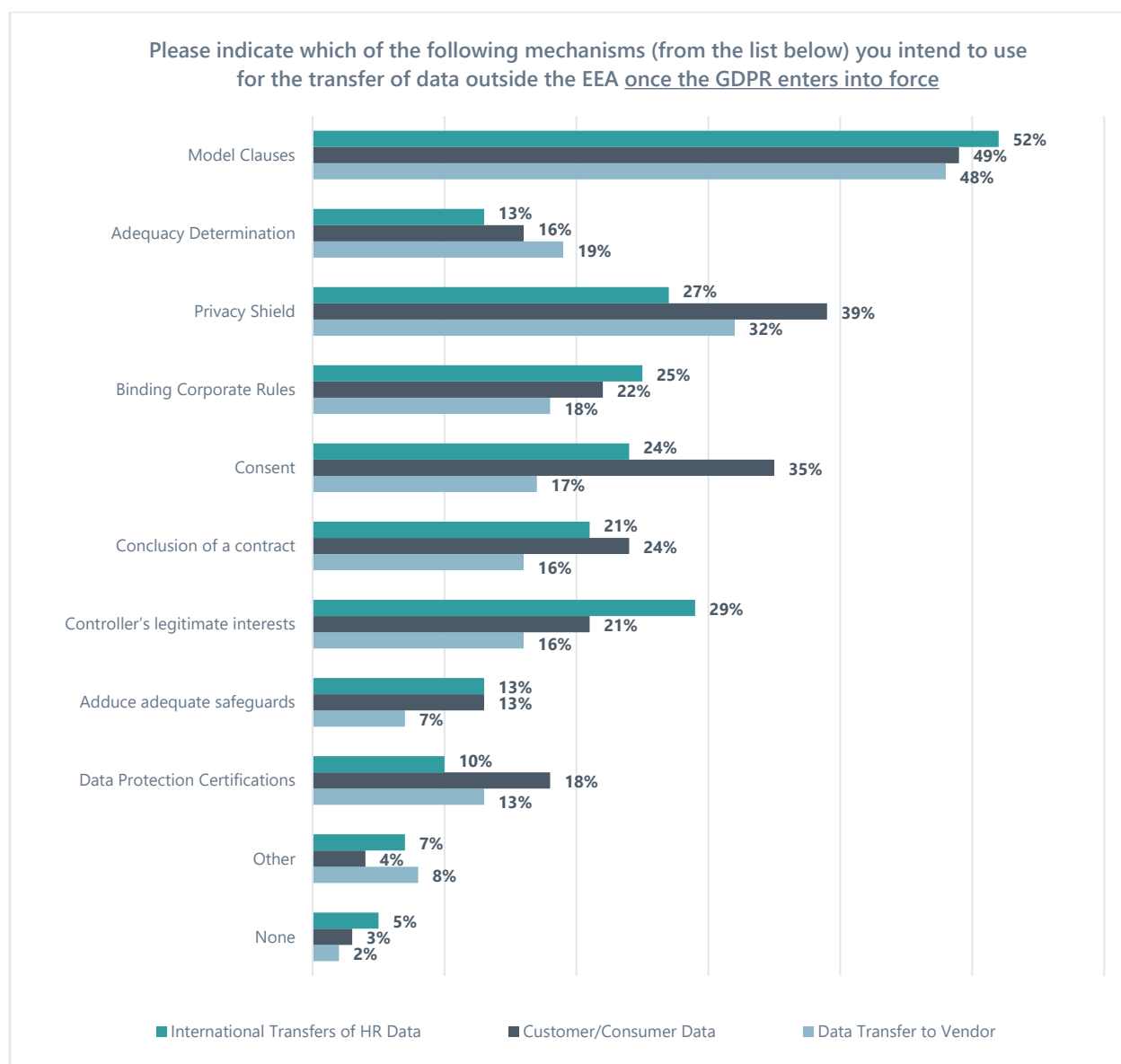
Organisations today use a wide variety of transfer mechanisms to legitimise data transfers outside the European Union, depending on the type and circumstances of the transfer. That trend will continue after May 2018. Despite the concerns discussed in the report in Section 1.3 above on the readiness to implement changes necessary to comply with the international data transfers provisions of the GDPR, more clarity is starting to emerge regarding different transfer mechanisms. This should increase confidence and uptake in certain transfer tools. For instance, the WP29 recently released updated working documents on elements and principles to be found in binding corporate rules for controllers and processors,<sup>6</sup> an updated adequacy referential<sup>7</sup> and guidelines on the Article 49 derogations for transfers.<sup>8</sup> Additionally, the European Commission released their report on the first annual Privacy Shield review in October 2017.<sup>9</sup>

The 2017 survey results show that:

- a. Model clauses remain the current most popular transfer mechanism for international transfers of internal HR data, consumer/customer data and data transfers to vendors. This is followed by consent (especially relevant for customer data, and not surprisingly less so for employee data), the Privacy Shield and necessity of contract.

- b. Post-GDPR, slightly more organisations will rely on the use of model clauses compared to the 2016 results which showed that slightly fewer organisations would rely on this mechanism post 25 May 2018.
- c. Most organisations are using binding corporate rules (BCR) today (13-16%) compared to 2016 (8-13%). As with the 2016 results, this is set to increase even further post-GDPR with 18-25% of organisations reporting they will use the transfer mechanism once the GDPR comes into force.
- d. Usage rates for the Privacy Shield are set to increase, with 18-30% of organisations reporting they currently rely on the Shield to transfer data and 27-39% reporting they intend to use the Shield post 25 May 2018. This is a significant increase on reported rates for Privacy Shield usage post 25 May 2018 in the 2016 survey (between 21-27% of organisations).
- e. Despite there being little information at this stage surrounding how adequate safeguards and data protection certifications will enable transfers under the GDPR, for the second year in a row respondents indicated they are likely to use these mechanisms, with 7-13% reporting they will use adequate safeguards and 10-18% reporting they will use certifications. In a recent communication<sup>10</sup> by the European Commission to the European Parliament and the Council, the Commission stated that it plans to look into GDPR certifications based on a study contracted with external experts and input from a multi-stakeholder group it set up in 2017. Given the interest in this mechanism, it is likely these rates will increase once there is more clarity surrounding certifications and their use in practice.





## 9. Breach Notification

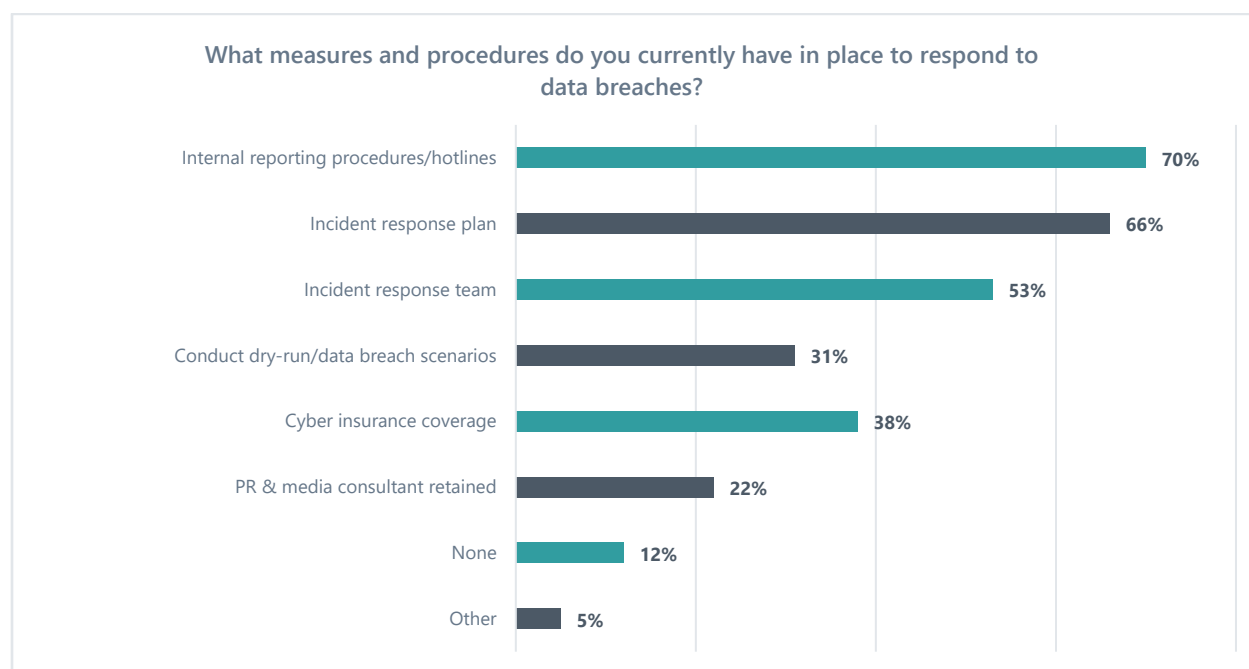
Preparedness levels in terms of breach notification vary widely. Encouragingly, almost 70% of organisations report that they have internal reporting procedures and hotlines in place and two thirds of organisations have incident response plans in place. 53% of organisations report they have a dedicated incident response team.

However, organisations still need to work on implementing several measures and procedures. Just under a third of respondents reported that they conduct dry runs and under a quarter retain PR and media



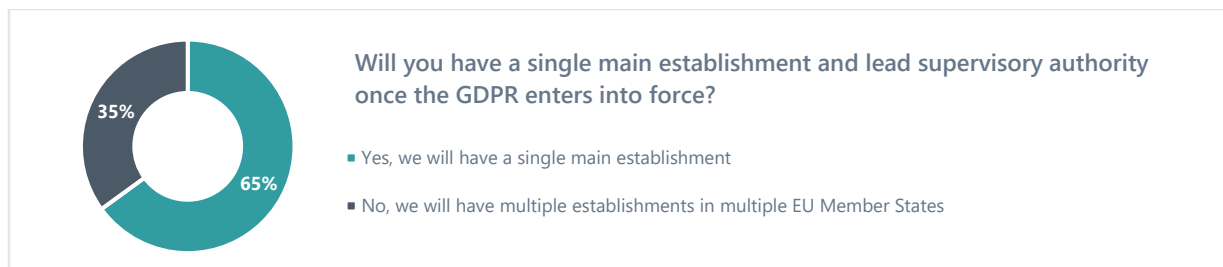
consultants. Encouragingly, it seems that more organisations are taking steps to secure cyber insurance, with almost two fifths of organisations reporting they have procured such coverage (38%).

Given the rise of cyber-attacks in the modern information age and new security breach notification requirements under the GDPR, along with serious penalties for failing to properly handle breaches, organisations will have to prioritise this work ahead of 25 May 2018.



## 10. Main Establishment

According to the 2016 survey, the majority of respondents reported they were confident in their ability to determine their main establishment and lead supervisory authority under the GDPR (77%). In 2017, we asked respondents whether they would have a main establishment and lead supervisory authority once the GDPR comes into force. Interestingly, about two thirds of survey respondents reported they will have a main establishment, with just over a third reporting they will have multiple establishments in multiple EU Member States. This makes it clear that there is a significant proportion of organisations that will be able to benefit from the main establishment and lead supervisory authority provisions of the GDPR.

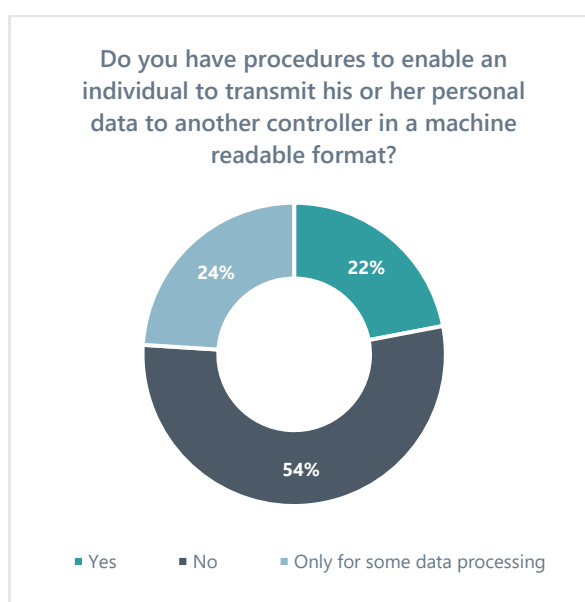
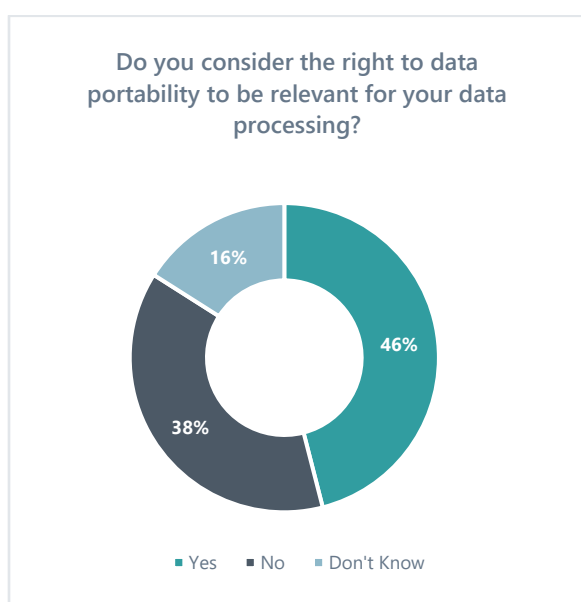


## 11. Right of Data Portability

Article 18 of the GDPR introduces the right of data portability allowing individuals to receive their personal data in a structured, commonly used and machine readable format and to have the right to transmit the data to another controller. Along with consumer empowerment, opportunities for innovation and sharing between controllers are key benefits of the newly introduced right.

Nevertheless, the 2017 survey results show that there continues to be confusion around the application of this right to organisations, with 54% of respondents reporting they do not consider the right of data portability to be relevant to them, or are unsure whether it is. This is slightly lower than 2016 (56%). These figures seem to indicate that organisations are still waiting to see how this right will be implemented and whether it will be widely used in respect of their specific processing of data.

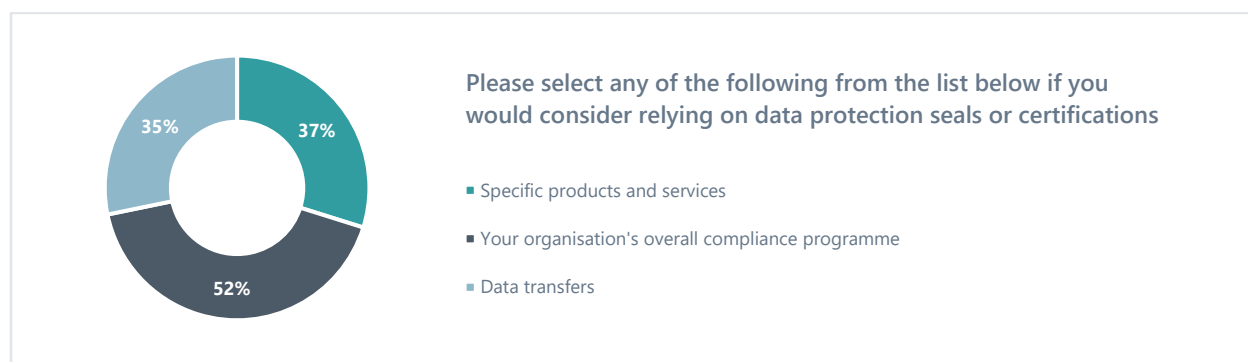
Encouragingly, many more organisations (22%) are implementing procedures to enable an individual to transmit his or her data to another controller in a machine readable format. This is a positive increase compared to 2016 when only 10% of respondents reported having such procedures in place. Still, 54% of organisations report that they do not have the required transmission procedures in place, which is consistent with the fact that many are unsure of if and how this right will apply in their specific context.



## 12. Seals & Certification

The GDPR encourages the establishment of data protection seals and certifications to demonstrate compliance and also serve as a mechanism for data transfer outside the EU. As indicated in Section 8, in a recent communication<sup>11</sup> by the European Commission to the European Parliament and the Council, the Commission stated that it plans to look into GDPR certifications based on a study contracted with external experts and input from a multi-stakeholder group it set up in 2017.

In 2016, 41% of respondents viewed certifications as being able to demonstrate their organisation's overall data privacy compliance programme. In 2017, over half of respondents (52%) reported they would rely on certifications to demonstrate their compliance programme, which is a significant increase and sends a strong signal in terms of industry's readiness to embrace certifications at programme level, providing they relay benefits for them. 37% of respondents would rely on certifications for specific products and services and 35% would rely on them for data transfers — an increase from 21% in 2016.



# About the Centre for Information Policy Leadership



**BRIDGING REGIONS**  
**BRIDGING INDUSTRY & REGULATORS**  
**BRIDGING PRIVACY & DATA DRIVEN INNOVATION**

## **ACTIVE GLOBAL REACH**

**55+**

Member Companies

**5+**

Active Projects & Initiatives

**20+**

Conferences, Workshops & Events Annually

**5+**

Principals & Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

### **ABOUT US**

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton & Williams LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age



[Twitter.com/the\\_cipl](https://twitter.com/the_cipl)



<https://www.linkedin.com/company/centre-for-information-policy-leadership>



[www.informationpolicycentre.com](http://www.informationpolicycentre.com)



2200 Pennsylvania Ave NW, Washington, DC 20037





Park Atrium, Rue des Colonies 11, 1000 Brussels, Belgium





30 St Mary Axe, London EC3A 8EP


# About AvePoint



  
Migrate

  
Manage

  
Protect



AvePoint, Inc. is headquartered and maintains its principal operational center in Jersey City, NJ, with approximately 1,500 employees across five continents.

15K

Customers

5M


Cloud Users

88


Countries

5

Continents



### From Tahoe to Today



- 2017 Partner of the Year Winner  
Public Sector: Microsoft CityNext Award
- 2016 Partner of the Year Winner  
Technology for Good Citizenship Award
- 2015 Partner of the Year Winner  
Collaboration and Content
- 2014 Partner of the Year Winner  
Public Sector: Public Safety and National Security

Inc. Magazine  
Hire Power Award

Windows IT Pro  
Best SharePoint Product

Ernst & Young  
Entrepreneur of the Year

Deloitte  
Technology Fast 500

# Glossary & References

## Glossary

**Controllers and Processors:** Controllers are the organisations that determine the means and purposes of data processing; processors are the organisations that provide data processing services to controllers, such as IT vendors or marketing firms.

**Binding Corporate Rules (BCR):** Binding and enforceable data privacy rules for intra-group, cross-border data transfers that are binding on all employees and all entities across the corporate group and that create a high and uniform level of data privacy across the group. Must be approved by lead data protection authority.

**Legitimate Interest Processing:** As lawful basis for processing where the processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject. Consent is not required where the legitimate interest ground for processing is met.

**One Stop Shop:** One single EU Data Protection Authority, the “Lead DPA”, serving as the “sole interlocutor” of a controller or processor concerning their cross-border processing matters in the EU. The lead DPA works with other concerned DPAs to ensure consistent application of the GDPR to the organisation.

## References

---

<sup>1</sup> <https://www.informationpolicycentre.com/global-readiness-benchmarks-for-gdpr.html>.

<sup>2</sup> WP251 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, [http://ec.europa.eu/newsroom/article29/document.cfm?doc\\_id=49826](http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826).

<sup>3</sup> WP250 Guidelines on Personal data breach notification under Regulation 2016/679, [http://ec.europa.eu/newsroom/article29/document.cfm?doc\\_id=49827](http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827).

<sup>4</sup> WP259 Guidelines on Consent under Regulation 2016/679, [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48849](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849).

<sup>5</sup> WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=47711](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711).

<sup>6</sup> See WP256 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48798](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798) and WP257 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48799](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799).

<sup>7</sup> See WP254 Adequacy Referential (updated), [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48827](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827).

<sup>8</sup> See WP262 Guidelines on Article 49 of Regulation 2016/679, [http://ec.europa.eu/newsroom/article29/document.cfm?doc\\_id=49846](http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846).

<sup>9</sup> First annual review of the functioning of the EU–U.S. Privacy Shield, [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=47798](http://ec.europa.eu/newsroom/document.cfm?doc_id=47798).

<sup>10</sup> See Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf).

<sup>11</sup> See Footnote 10.