AvePoint®

Centre for Information Policy Leadership
Hunton & Williams LLP

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

Contents

Foreword

Bojana Bellamy
President, Centre for Information Policy Leadership

The GDPR signals the start of a new generation of data privacy laws and practice in Europe and beyond. The new law will bring changes to data privacy authorities, who will have to work in a new, consistent, and coordinated manner across Europe; to individuals, who will feel more empowered with enhanced rights, transparency, and redress; and to organisations, which will have to address the commercial, business, and legal impact of the new rules on the way they use and manage data, their data strategy, their IT systems and infrastructure, and how they engage with regulators and individuals. This GDPR impact and readiness survey report is designed to help organisations understand and benchmark the key operational impacts of the regulation and to support their internal change management program, as they drive forward with implementation ahead of the May 2018 deadline.

Dana Simberkoff
Chief Compliance and Risk Officer, AvePoint

The EU GDPR imposes not only significantly greater fines for data breaches, but also mandates a major shift for many organisations, even those that already have a privacy programme. New obligations for the CIO, CISO, and the business mean that those waiting for the law to come into effect are already too late to comply. 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. 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) will bring significant changes to how companies manage and process personal data, their privacy compliance programmes, as well as IT systems and infrastructure. The GDPR replaces Directive 95/46/EC (the Directive) and will come into force in May 2018.

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. The objective of the survey was to help organisations benchmark and prepare their GDPR implementation and change management programmes.

Our questions focused on key change areas and topics of the GDPR that relate the most to everyday business and compliance concerns.

The survey respondents totalled 223, with predominantly multinational organisations. According to respondents, 93 percent of organisations operate in Europe, more than half operate in the US, and less than half in South America and Asia. Telecommunication and technology companies were the most highly represented of the total respondents, followed by insurance and financial services, as well as pharmaceutical and healthcare sectors. The survey respondents were a mix of both controllers and processors with slightly more controllers (57 percent controllers; 43 percent processors). Finally, organisations' annual revenue size ranged from less than $1 million to more than $100 billion.

The survey reveals that most companies have started the process of assessing the impact of the GDPR on their operations, devising a company-wide implementation plan, and evaluating the need for additional resources. We observed the following key trends:

1. **GDPR Impact:** Respondents believe that the aspects of the GDPR that will have the largest impact on their organisations are the requirements for a comprehensive privacy management programme, use and contracting with processors, as well as data security and breach notification. As expected, senior management is most concerned about the GDPR's enhanced sanction regime and the data breach notification requirements, as well as how the regulation will impact their data strategy and ability to use data.

2. **GDPR Readiness:** Organisations appear to be in the varying stages of preparation for the GDPR. While most have appointed a data protection officer (DPO), many organisations are either increasing resources in preparation, or are in the process of considering additional resources to meet the increased obligations under the GDPR.

3. **Consent and Legitimate Interest:** At present, companies collecting personal data rely heavily on consent of individuals, but only a minority would be able to meet the enhanced requirements for consent under the GDPR using their current methods. Almost one third of organisations say they will rely more on the legitimate interest processing legal basis under the GDPR than they currently do.

4. **Data Privacy Impact Assessment (DPIA) and Privacy by Design:** The majority of organisations already carry out, or are preparing to carry out, DPIAs in the circumstances defined by the GDPR. More than 36 percent of organisations have a framework to identify risks to individuals, with another 36 percent working on developing such a framework. The vast majority of companies tend to incorporate privacy and security by design into the development of new products/services regularly or some of the time.

5. **Controller - Processor Relationship and Agreements:** A majority of organisations' standard processing agreements already reflect some of the new GDPR requirements. This could explain the fact that review or renegotiation of current processing agreements is not widespread, with only 32 percent of organisations currently undertaking such a review or renegotiation. Separate from the contractual requirements, processors will be most impacted by the GDPR requirement to document all data processing activities and adhere to the restrictions on data transfers outside the EU.

6. **Data Transfers Outside the EU:** Organisations appear to use a wide variety of mechanisms today for data transfer related to internal human resources (HR), consumers/customers, and vendors. According to responses, they will continue to do so after the GDPR is implemented. The most popular mechanisms today are, in descending order: Model Contracts, consent and necessity for contracts, as well as Privacy Shield. After the GDPR is in place, in addition to Model Contracts, there is expected to be an increased use of binding corporate rules (BCR), the legitimate interest processing derogation, and Privacy Shield.

7. **Security Breach Notification:** The majority of companies have a procedure for reporting breaches as well as an internal response plan and team. This will enable them to comply with the new requirements for notifying data protection authorities (DPAs) and individuals affected in the wake of a breach. However, unlike in the US where breach notifications are mandatory in almost every jurisdiction, only a minority of organisations conduct "dry runs" of their breach notification plans, have cyber insurance, or retain public relations and forensic experts.

8. **Compliance Technology Tools and Software:** Currently, organisations do not appear to use widely, or have access to, technology tools and software to aid data privacy compliance tasks. Only a minority of organisations use technology to automate and industrialise their DPIAs, data classification and tagging policies, data processing inventories, and delivery of the new data portability right.

9. **Joined up Approach to GDPR Implementation:** Because of interdependences between data privacy compliance, IT systems and infrastructure, and organisations' data strategy, GDPR implementation should be a company-wide change management programme, with a concerted effort from senior leadership, including DPO, CISO, CIO, CDO and GC.

Survey Results and Key Findings

1. GDPR impact, organisational readiness, and resources

1.1 Key areas of impact and senior management focus

Respondents have identified the following three areas where the GDPR will have the highest impact on their organisation and compliance:

a) Privacy programme management
b) Use and contracting with processors
c) Data security and breach notification

These are the areas of the GDPR that require the most operational changes. Organisations will have to build and maintain comprehensive privacy compliance programmes, verify them internally or externally and be able to demonstrate the existence and effectiveness of their programmes.

Additionally, the new requirements for breach notification to supervisory authorities and individuals affected will require new policies and procedures as well as increase the risk profile for organisations. Unsurprisingly, the survey results also showed that, together with the enhanced sanction regime, this is the area of highest concern for senior management.

Finally, the new GDPR obligations on processors and requirements for processing contracts, with joint liability, will require considerable implementation effort. This may range from a review of standard terms and contracting practices both for existing and future processing contracts, to the impact on commercial terms and negotiations in the future.

Please rate the impact that the following new GDPR requirements will have on your organisation.

Compliance Area	Minimal Impact	Medium Impact	High Impact
Core Processing Principles	42%	27%	30%
Individual Rights	37%	33%	31%
Privacy Programme Management	21%	31%	**49%**
Use and Contracting with Processors	27%	29%	**44%**
New Obligations on My Organisation as Processor	44%	24%	32%
Data Security and Breach Notification	34%	26%	**41%**
Internal Data Transfers	44%	23%	33%

In addition to enhanced sanctions and data breach notification requirements, senior management was

also concerned about the GDPR's stricter rules on consent and the impact on the organisations' ability to use and re-use data. This confirms the fact that GDPR and data privacy compliance are closely related to a company's data strategy, big data and analytics, and data-driven innovation. It also supports the fact that data is critical to many business processes, products, and services. This is why GDPR implementation must be a concerted effort across the organisation, with the DPO working hand-in-hand with Chief Data Officer (CDO), Chief Information Officer (CIO), Chief Information Security Officer (CISO) and other senior leadership.

Senior Management Concerns about the GDPR

Compliance Area	Not Concerned	Process Underway	Highly Concerned
Additional Processing Obligations	37%	32%	30%
Changes to Internal Privacy Programme	33%	34%	33%
Data Security Breach Reporting	26%	36%	38%
Enhanced Individual Rights	32%	35%	33%
Enhanced Sanctions Regime	27%	28%	**45%**
Internal Data Transfers	39%	29%	32%
Restrictions on Profiling	37%	35%	28%
Stricter Rules on Reuse of Data	31%	35%	34%

1.2 Readiness for change

Respondents seem to be in varying stages of readiness in respect of implementing different GDPR compliance areas, with less than one third feeling fully or nearly compliant with key aspects of GDPR.

The organisations appear to be least ready in respect of legal and operational changes relating to:

a) Privacy programme management
b) Individual rights
c) Use and contracting with processors

For example, only 22 percent feel fully ready or near to fully ready for implementing the GDPR requirements in respect to their privacy programmes.

Of course, companies will feel more ready for certain aspects of GDPR compliance than others. Respondents appear to be less confident about newer requirements and obligations, such as individuals' rights, which have expanded under the GDPR. Only 24 percent of respondents felt they were either fully compliant or near to full compliance, with the majority of respondents feeling a low-to-medium level of compliance. Equally, 43 percent of processors do not feel ready in respect to new obligations imposed by

GDPR.

Surprisingly, only 8 percent of respondents feel they are fully ready for implementing the GDPR requirements on international data transfers, with another 27 percent feeling they were nearly ready. This may reflect the mounting legal uncertainty around some of the existing transfer mechanisms and the fact that organisations will have to consider new mechanisms to justify different types of data transfers under the GDPR.

Please indicate how ready you consider your organisation to be for the following under the GDPR.

Compliance Area	Fully Compliant	Process Underway	Neutral
Core Processing Principles	30%	36%	35%
Individual Rights	24%	29%	**47%**
Privacy Programme Management	22%	35%	**43%**
Use and Contracting with Processors	24%	39%	37%
New Obligations on my organisation as processor	22%	35%	**43%**
Data Security and Breach Notification	37%	30%	33%
Internal Data Transfers	35%	32%	33%

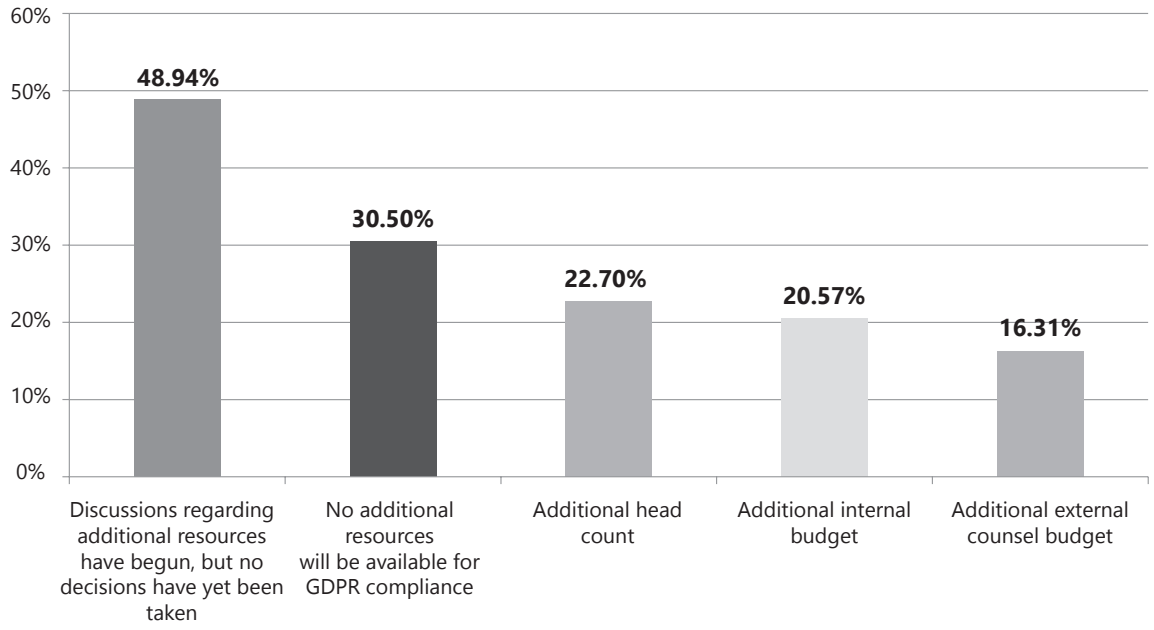
1.3 Impact on Resources

Given the two-year implementation deadline for GDPR compliance, organisations are already considering the impact of GDPR on their headcount, budget, and additional resources.

However, at close of the survey in September 2016, less than one fifth of organisations have actually committed either additional headcount, budget, or external counsel spend for GDPR implementation. Almost half of respondents are still in discussions regarding additional resources but have not yet made a decision. One would assume that these decisions will be made shortly, given the budgetary and planning cycles in most organisations, to enable full GDPR implementation by the May 2018 deadline. Approximately 31 percent of the respondents will not have any additional resources made available to them for GDPR compliance. This is somewhat concerning, but can also be interpreted to mean that the organisations have adequate resources already and their privacy programme is mature enough not to warrant too many changes.

Finally, the majority of organisations responding to the survey have already appointed a group or regional data protection officer, with only 15 percent not having this role at the time of response.

Do you have a budget, headcount, or other resource increase planned in anticipation of the GDPR?



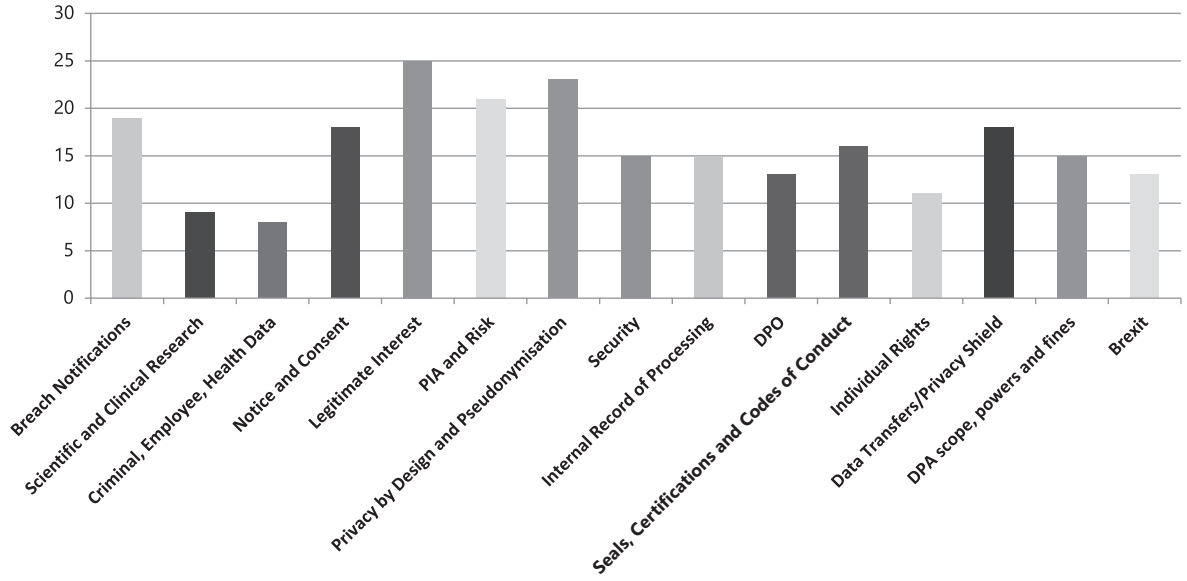
2. Further clarity on certain aspects of the GDPR

As with any change of law, it is not surprising that organisations are seeking additional guidance and clarification around the GDPR. Even though some of the GDPR concepts are the same as in the Directive (e.g. legitimate interest processing), the implementation, interpretation, and circumstances which apply will change.

Of about 40 survey respondents who answered this optional question, they prioritised the following three areas as requiring further clarification: (i) Legitimate interest (25 responses); (ii) Privacy by design and pseudonymisation (23 responses); and (iii) DPIA and risk (21 responses). They are closely followed by the topics of breach notification; notice and consent; and international data transfers.

The Article 29 Working Party (WP29) is due to issue guidelines on four areas of the GDPR in late 2016 or early 2017: DPIA and risk, DPO, data portability, and certifications. Other areas will follow in 2017 and 2018. While DPIA and risk will be the subject of guidance due in 2016 or early 2017, at this stage there is no indication of any WP29 guidance on the other topics identified by the survey respondents.

What areas of the GDPR require further clarity for your organisations?



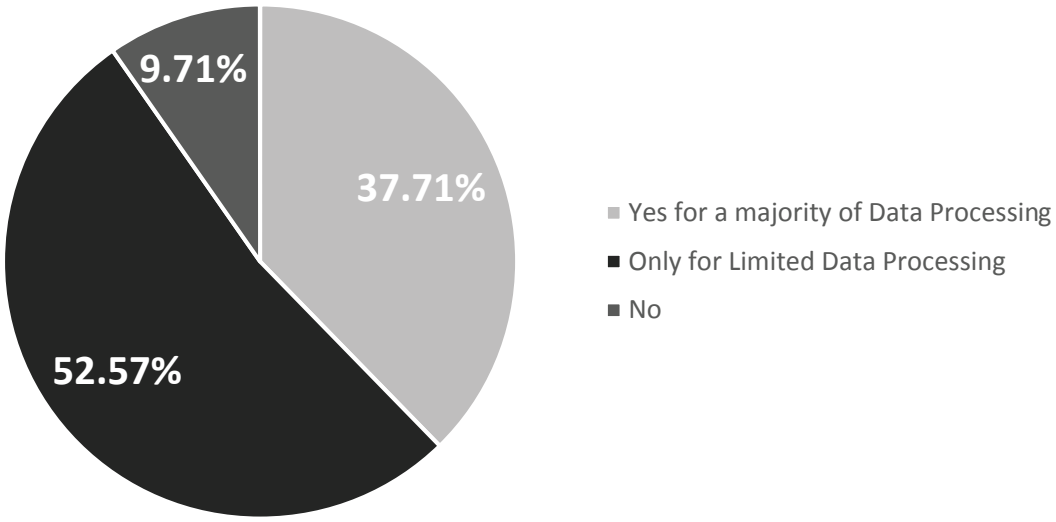
3. Consent and legitimate interest

Consent remains a lawful basis to process personal data under the GDPR. However, the standard of consent is significantly higher than before. Whereas the Directive allowed controllers to rely on implicit and "opt-out" consent in some circumstances, the GDPR requires the data subject to signal agreement by "a statement or a clear affirmative action." In addition to being freely given, specific, informed, and an unambiguous indication of the data subject's wishes, consent under the GDPR will have to be documented; given for each specific processing operation and purpose; and "clearly distinguishable" from any other matters. Finally, consent can no longer be made a condition of using a service or a contract – hence, it will be unlikely to form part of standard terms and conditions.

3.1 Processing based on consent

The survey results indicate that organisations today use consent widely across a spectrum of processing operations, with 38 percent using consent for the majority of their processing and 53 percent for limited processing.

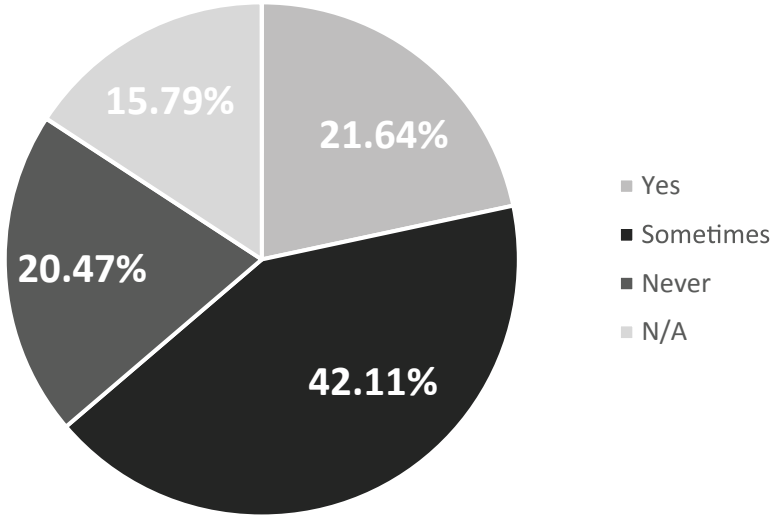
Do you rely on consent to process personal data?



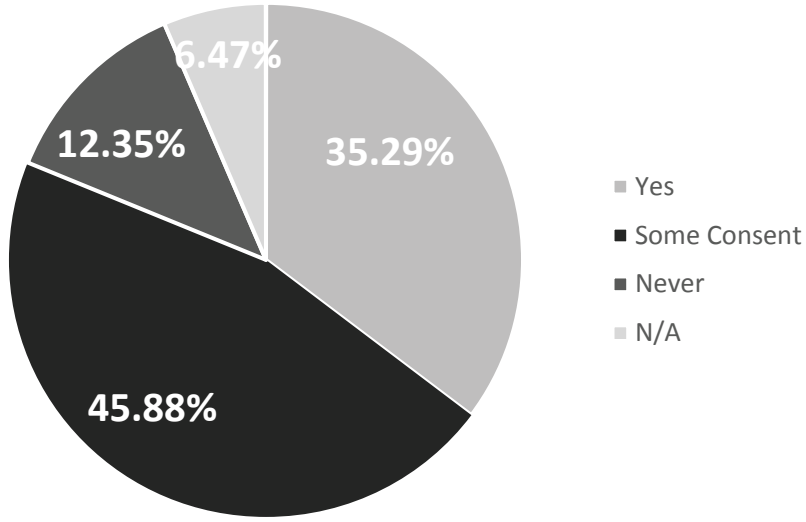
However, the survey shows that only one third of organisations are currently fully able to comply with the enhanced consent requirements of the GDPR.

- Just over one fifth (22 percent) currently gather a separate consent for each processing activity.
- Only one third (34 percent) are able to demonstrate that consent was validly given.
- Three quarters (76 percent) either always or sometimes make the consent they obtain from individuals conditional upon use of a product or service offered.

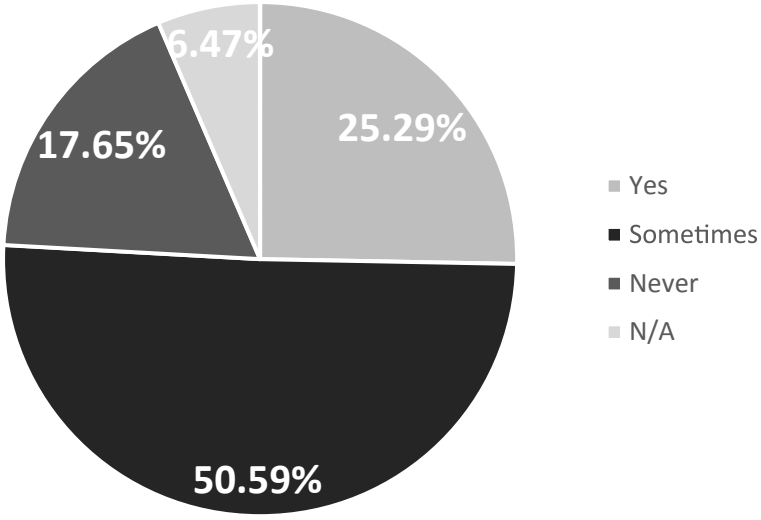
Do you obtain separate consent for different processing operations?



Do you have processes in place to enable you to demonstrate consent was validly given in any particular case?



Do you require individuals to consent to the processing of personal data as a condition of using a product/service?



These results show that, in preparation for the GDPR, most companies will need to undertake a full review of the content of, and mechanism for obtaining, individuals' consent per data processing activity. Depending on the nature of a company's data processing activities, such a review may require significant changes to websites and forms, terms and conditions (T&Cs), privacy policies, and other consent mechanisms. It seems highly likely that existing consent processes will need to be refreshed, both in terms of the mechanism for obtaining consent as well as the information provided to individuals when carrying

out the process. As we note below, given the more stringent requirements for consent, companies are turning to alternative legal bases to legitimise their processing activities.

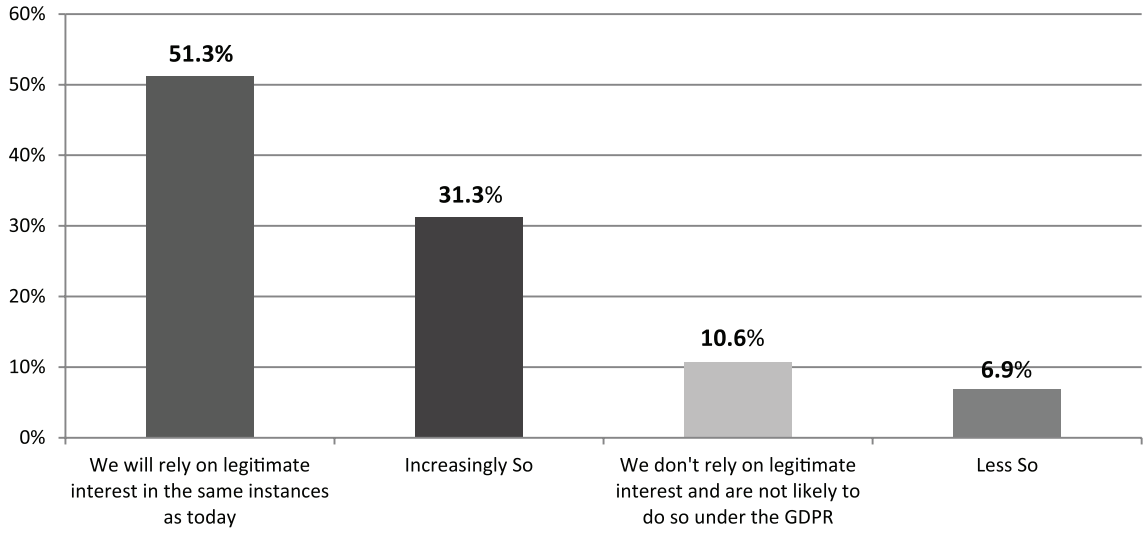
3.2 Legitimate interests processing

Under the GDPR, the legitimate interests of a controller, or a third party, can be used as a legal basis to process personal data, just like the consent of individuals.

The survey showed that just under a third of respondents (31 percent) will consider using legitimate interests more as a legal basis for processing under the GDPR. This observation is perhaps not surprising given the higher standard for consent under the GDPR. Also, with the ubiquitous data processing in this digital era as well as connected and smart devices, it is not surprising that reliance on consent from individuals is simply not going to be realistic, and it may overburden individuals as they go about their life and work. It would not be surprising if legitimate interest becomes a more prevailing grounds for processing – albeit still subject to strict conditions and balancing tests that require organisations to assess the impact on and any risks and harms to individuals.

However, it is important to note that, under legitimate interest processing, organisations will still have to be accountable and undertake the full process of assessing the legitimate interest and then balancing that with the rights and freedoms of individuals. They will also have to include the explanation of legitimate interest in the notice to individuals, the substance of these interests, and how they do not override the interests of the individuals. Finally, related to this is the reversal of the burden of proof in relation to the right to object to processing, which will mean that where personal data is processed under the legitimate interest basis, if an individual objects, such an objection must be upheld unless the controller has compelling legitimate reasons for processing the personal data.

Do you intend to rely on legitimate interests as a condition for data processing once the GDPR enters into force?



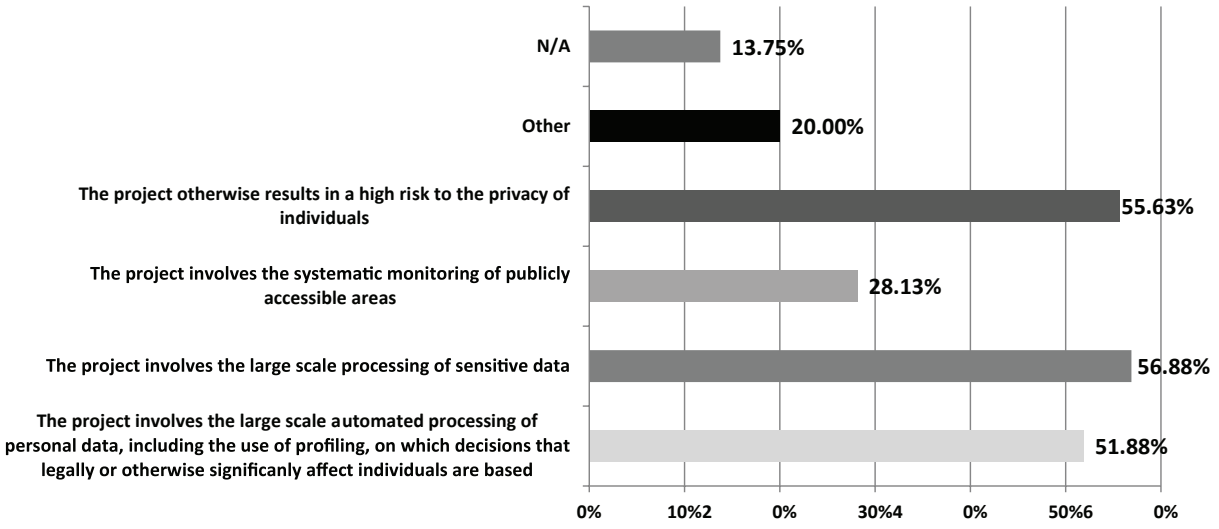
4. Data Privacy Impact Assessments (DPIAs) and privacy by design

4.1 Data Privacy Impact Assessments

Under the GDPR, companies will have to conduct formal DPIAs in relation to any processing that would result in "high risk" for individuals' rights and freedoms. The notion of high risk is not defined in the GDPR, but there are three examples of high risk processing: (i) the large scale processing of sensitive personal data; (ii) automated decision taking; and (iii) systematic and large scale monitoring of publicly accessible areas.

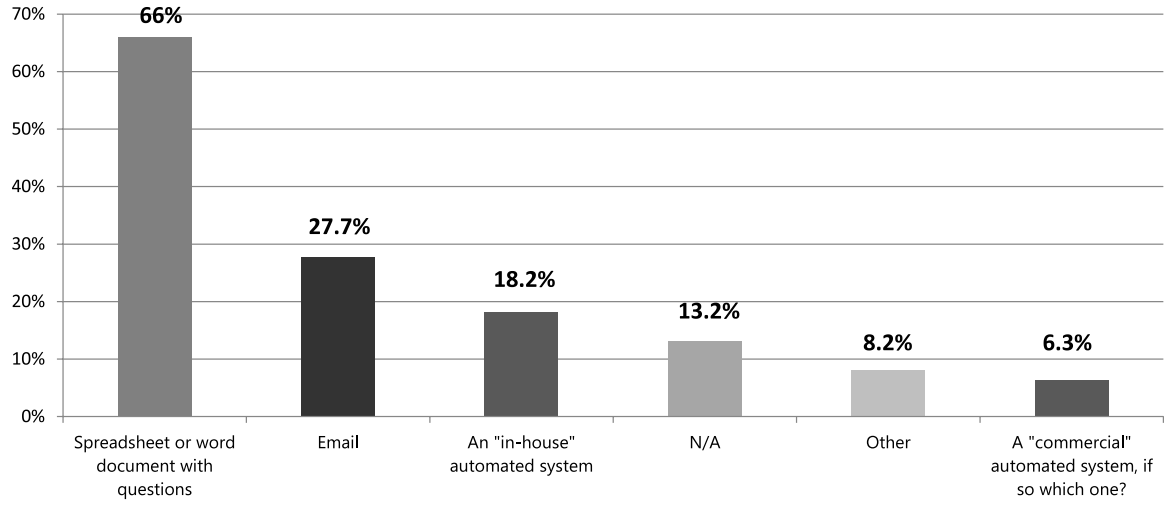
The survey results showed that 52 to 57 percent of organisations already carry out DPIAs in circumstances envisaged by the GDPR (other than in relation to the monitoring of publicly accessible areas, where only 28 percent conduct DPIAs). This likely demonstrates the benefits that DPIAs have in detecting data privacy risks when developing products, services, and technologies.

Do you conduct DPIAs in any of the following circumstances?



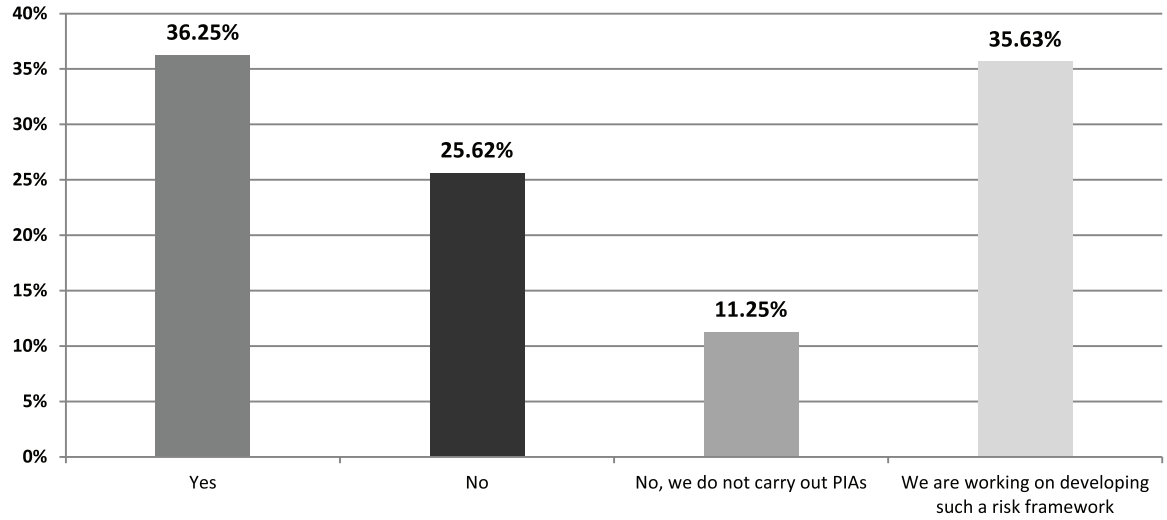
While there is a growing best practice in carrying out DPIAs, the actual process is more ad hoc or informal in nature. This is supported by the fact that 66 percent of DPIAs that are carried out currently are in programmes like Word and Excel while 28 percent are by email. Only 18 percent of organisations use an in-house built automated system and another 6 percent use a purchased/commercial automated system. It is likely that this number will grow as more commercial tools and software become available on the market to support DPOs as well as enable industrialisation and automation in meeting GDPR compliance.

If you carry out DPIAs, which method(s) do you use?



The formal methodology of DPIAs within organisations, however, is not clear. It is encouraging that 36 percent of organisations already have a framework in place to identify and assess the risks to individuals, and a similar number have already started work on developing such a framework. 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. Under the GDPR, risk assessments will become an integral part of privacy management programmes, and will enable organisations to calibrate compliance based on the likelihood and severity of risks to individuals.

When carrying out DPIA's, do you have a procedure or framework to identify and classify different risks to individuals?



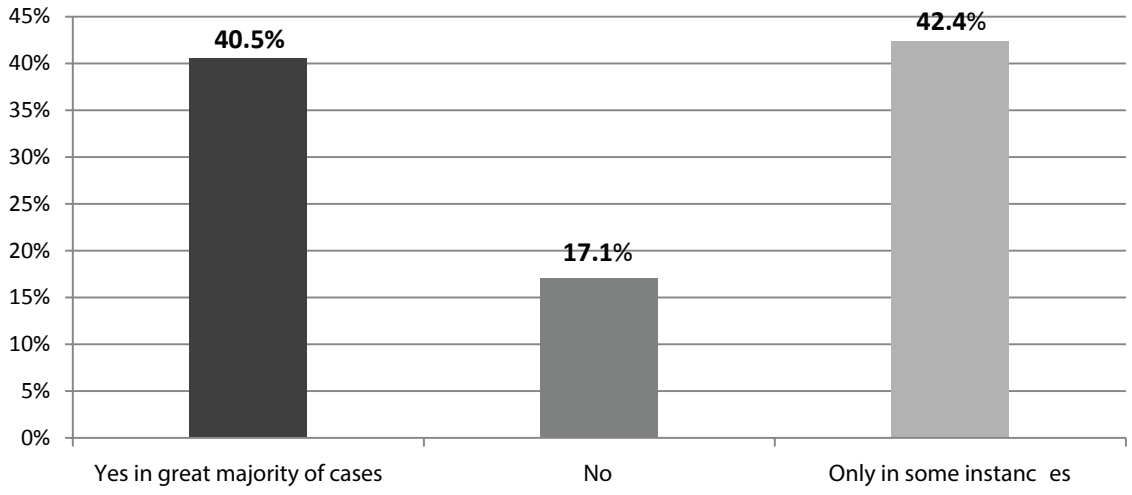
4.2 Privacy by Design

The GDPR puts forth "Privacy by Design" as one of the many obligations that require interconnection between the different roles and functions in organisations, including the DPO, CISO, IT team, and CIO. The GDPR requires not only privacy and security by design, but also "by default." This means that what was formerly considered to be "best practice" will now be a mandate that needs to be operationalised.

Data privacy and security requirements must be embedded within the development of products, services, and technologies throughout the whole process – from the planning stage of a new IT project, programme, or system, through the design, development, quality assurance, and release.

It is encouraging to see organisations implementing privacy by design principles in the development and roll out of new products, services, and technologies. Almost 41 percent of survey respondents regularly incorporate privacy by design in the development of new products/services, and another 42 percent in some instances only. With GDPR requiring organisations to ensure compliance at the time of both system design and implementation, organisations will be well placed to comply with this new legal requirement.

Do you incorporate 'privacy by design' principles in the development and roll-out of new projects that involve the use of personal data?



5. Controller - processor relationship and agreement

Under the Directive, the outsourcing of data processing operations required the controller to execute a written agreement with the processor. The agreement contained basic requirements stating the processor could only act on behalf of the controller and implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. The processor's main obligations stemmed from the contract with the controllers, and the controller was responsible for data protection compliance under the law.

The GDPR has brought real changes to the relationship between controllers and processors and to the status of processors themselves. Firstly, the processors are now subject to GDPR obligations, including data security, data transfers outside the EU, appointment of a DPO, maintaining record of processing activities, and cooperating with DPAs. Also, the list of compulsory provisions to be included in the data processing agreement between a controller and processor has been expanded. The processing agreement must include provisions related to:

- Confidentiality
- Rights of data subjects
- The obligation for the processor to provide assistance to a controller in respect of regulatory queries
- The obligation on a processor to make information about the processing it carries out available to a controller
- The requirement for a processor to notify the controller about breaches related to the restriction on sub processing without a controller's consent
- The controller's right to audit the processor

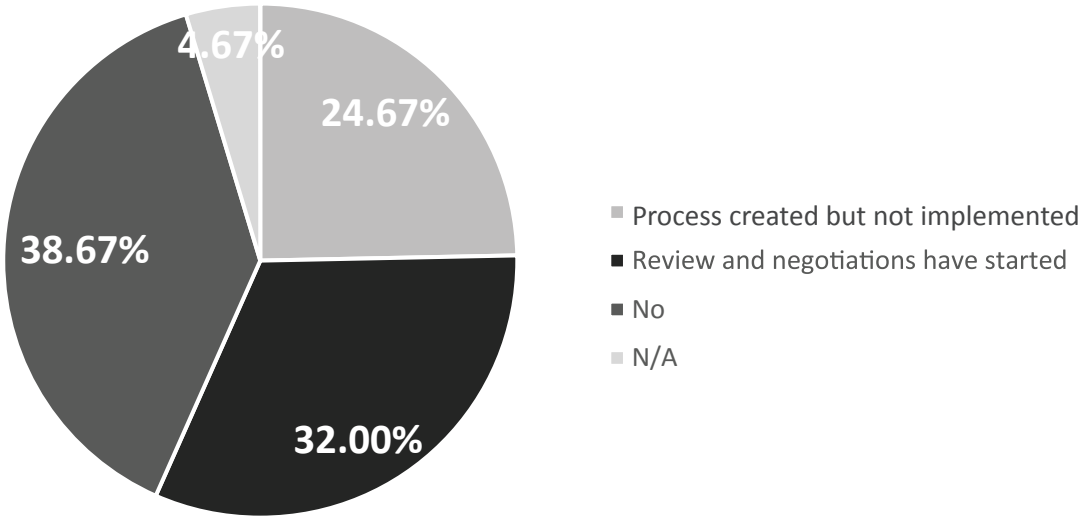
Finally, processors may be pursued in courts and liable vis-à-vis individuals for any breaches under the GDPR.

5.1 Controller – processor agreements

The changes to the contractual terms for data processing agreements will require considerable efforts on the part of both controllers and processors, both in respect of existing relationships and new ones. It may also lead to some unintended consequences, such as one of the parties using this as an opportunity to open up renegotiations in relation to the commercial terms.

Such a review and renegotiation process may be lengthy. In light of the fact there are no transitional provisions for existing processing agreements, it is not surprising that almost a third of organisations (32 percent) have already started this process. However, almost 40 percent have not commenced work on the review of standard processing terms and renegotiation of existing contracts.

Have you implemented a process to review and revise your standard processing terms, and review and, if necessary, renegotiate data processing agreements with third parties?



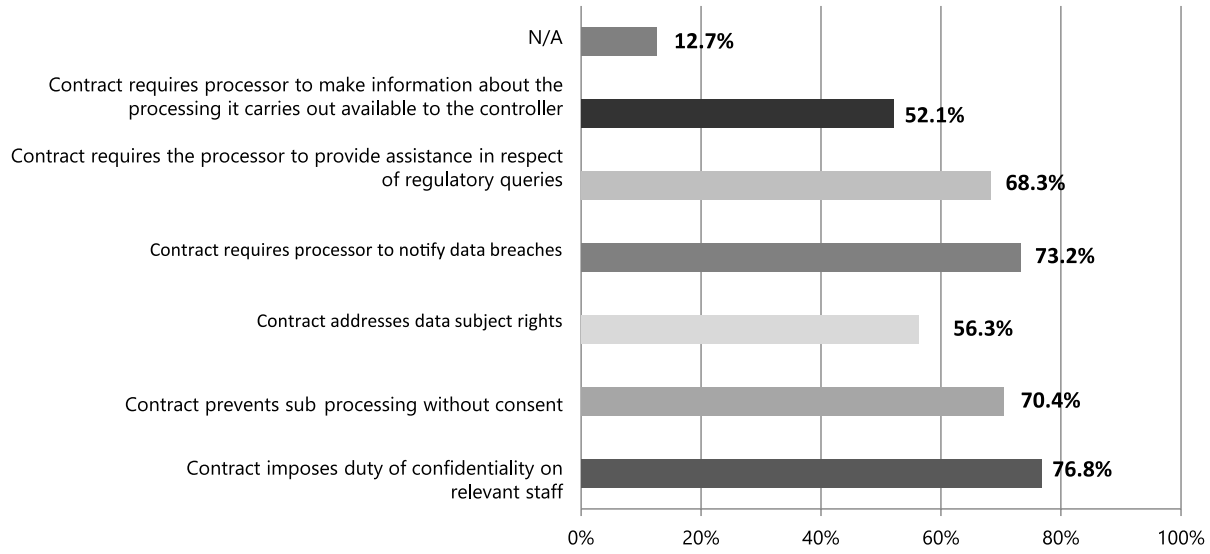
It may be that for some respondents, the additional contractual terms required by the GDPR are already included in their data processing contracts. In this case, changes will not be required or will be minimal. Interestingly, a majority of the respondents already include the newly required terms in their contracts, such as the requirements for the processor to:

- Notify the controller about any data breaches (73 percent)
- Impose a duty of confidentiality on relevant staff handling personal data (76 percent)
- Not sub-process without consent (70 percent)
- Provide assistance to a controller in respect of regulatory queries (68 percent)

This may be explained by the fact that specific Member State laws, such as those in Germany, already provide for stricter processing agreement requirements than were required by the Directive, and that these laws have set the bar for the European market.

On the other hand, some of the other new GDPR requirements are less present in current agreements. Just over a half of respondents currently address individuals' rights in their processing contracts (56 percent), or require processor to make information about the data processing available to the controller (52 percent).

Do your standard data processing terms include additional terms required by the GDPR?



5.2 Obligations for processors

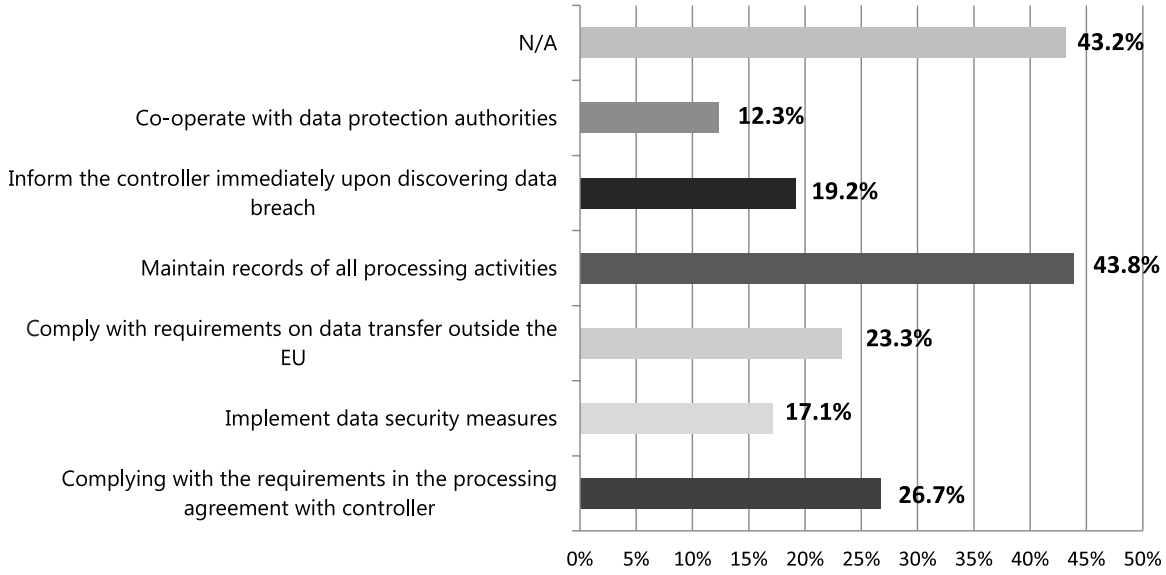
Under the GDPR, processors will, for the first time, have statutory obligations when they process personal data. The GDPR, therefore, is likely to have a major legal and commercial impact on processor organisations.

Survey respondents from processor organisations indicated that they would be most impacted by the GDPR in respect to:

(i) Documenting all data processing activities (43 percent),
(ii) Complying with the terms of the controller/processor agreements (27 percent)
(iii) Data transfers outside EU (23 percent)

Perhaps not as surprising was the lower change impact of the new requirement on processors to inform controllers of a data breach. This is consistent with the fact that almost three quarters of organisations (73 percent) already include data breach provisions and notification requirements in their data processing agreements (see question 35).

If your organisation is a processor, which of the additional obligations under the GDPR for processors will require most internal consideration and change for your organisation?



6. International data transfers

Under the GDPR, existing transfer restrictions under the Directive continue to apply and derogations are maintained. Additional derogations (such as legitimate interest for non-routine transfers) and new transfer mechanisms (such as BCRs and seals and certifications) have been included in the GDPR.

The survey data reveals the following key findings in respect of international transfers of internal HR data, consumer/customer data, and data transfers to vendors:

a) Today, organisations use a wide variety of mechanisms to legitimise data transfers outside the EU, depending on the type and circumstances of the transfers. That trend will continue after the GDPR comes into force. Organisations will welcome the fact that the GDPR provides for an even larger spectrum of transfer mechanism options.

b) The most popular mechanisms today appear to be the EU Model Clauses, used by two thirds of the respondents for all three types of data transfers. This will continue post-GDPR, with Model Clauses being most popular for data transfers to vendors (63 percent post-GDPR) and for transfers of HR and customer/consumer data (59 percent post-GDPR). Today, Model Clauses are closely followed by consent, necessity for the contract, and Privacy Shield, as the most popular transfer mechanisms.

c) BCR being formally recognised in GDPR is a welcome addition to data transfer mechanisms. It is not surprising, therefore, that the survey data shows a considerable increase for BCR post-GDPR. For the different types of data, 8-13% of organisations are

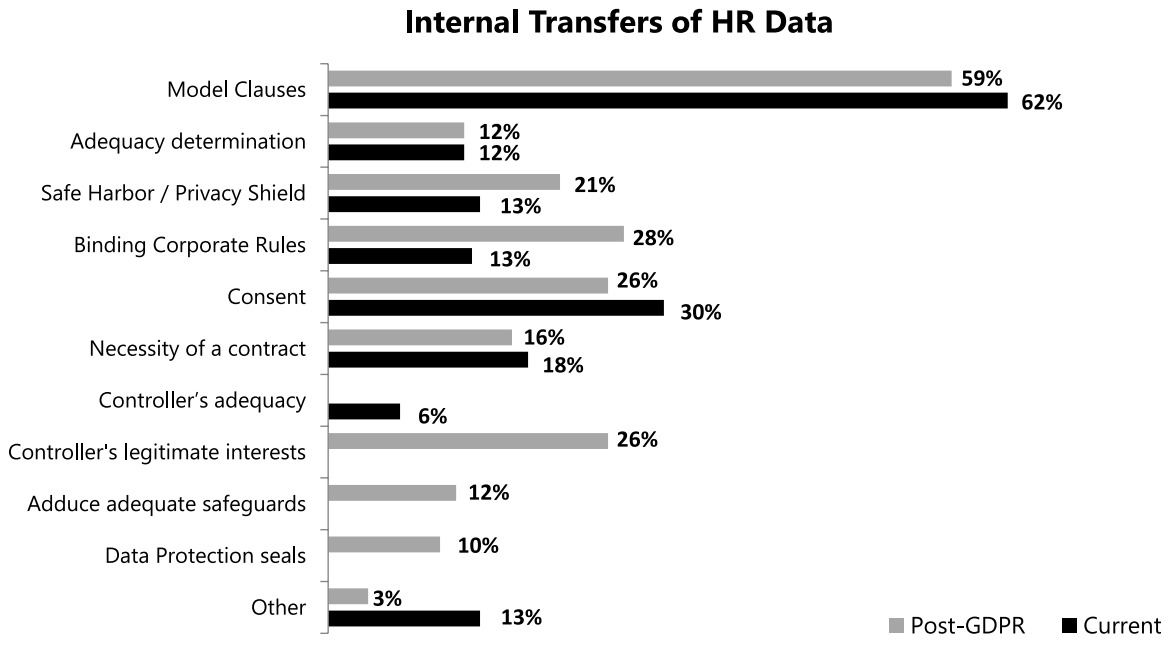
using BCR today. Post-GDPR, that number will increase to 28 percent for HR and customer/consumer data and 21 percent for data transfers to vendors. This reflects the growing popularity of BCR, as the approval process has become mainstream and the time to obtain approval from DPAs for BCR has been reduced over time. It also reflects, in particular, the number of service providers creating and using processor BCR since its introduction in 2013.

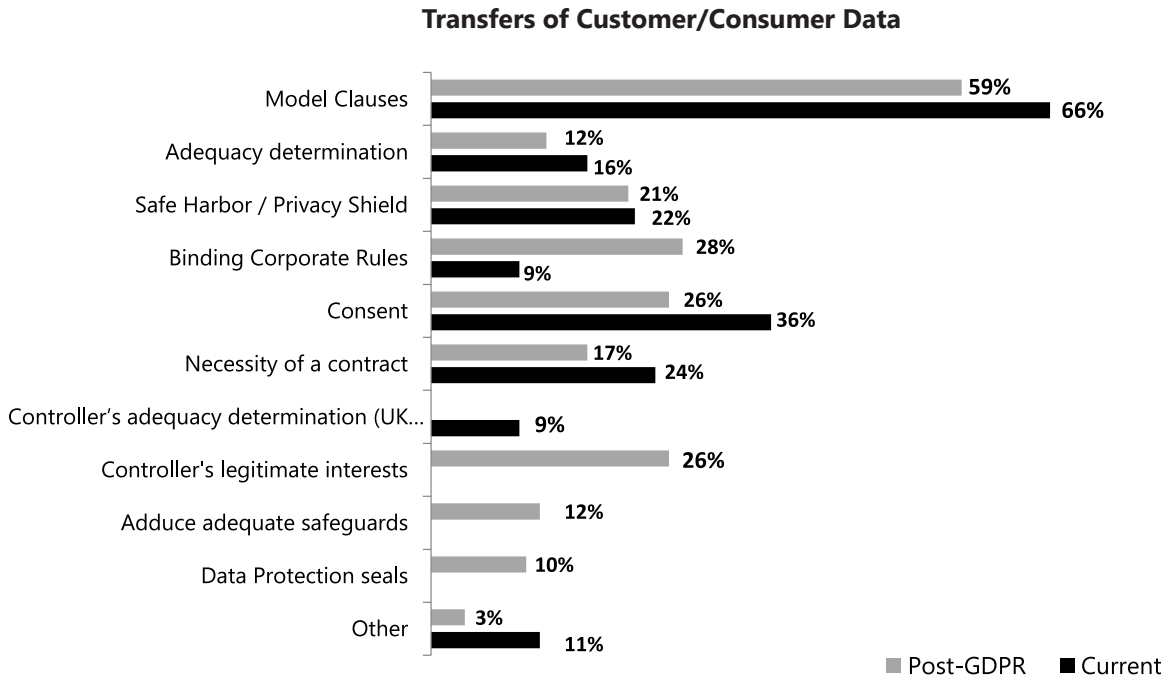
d) Post-GDPR, in addition to BCR, there will be more use of two other data transfer mechanisms. Between 21 and 27 percent of organisations will use Privacy Shield, and about a quarter of organisations use controllers' legitimate interest as a basis for international data transfers. Clearly, organisations have an increased confidence in the newly agreed upon Privacy Shield. On the other hand, the confidence in using legitimate interest may be a bit over-optimistic, as this is a narrowly interpreted derogation, intended to apply in very limited circumstances of non-routine data transfers.

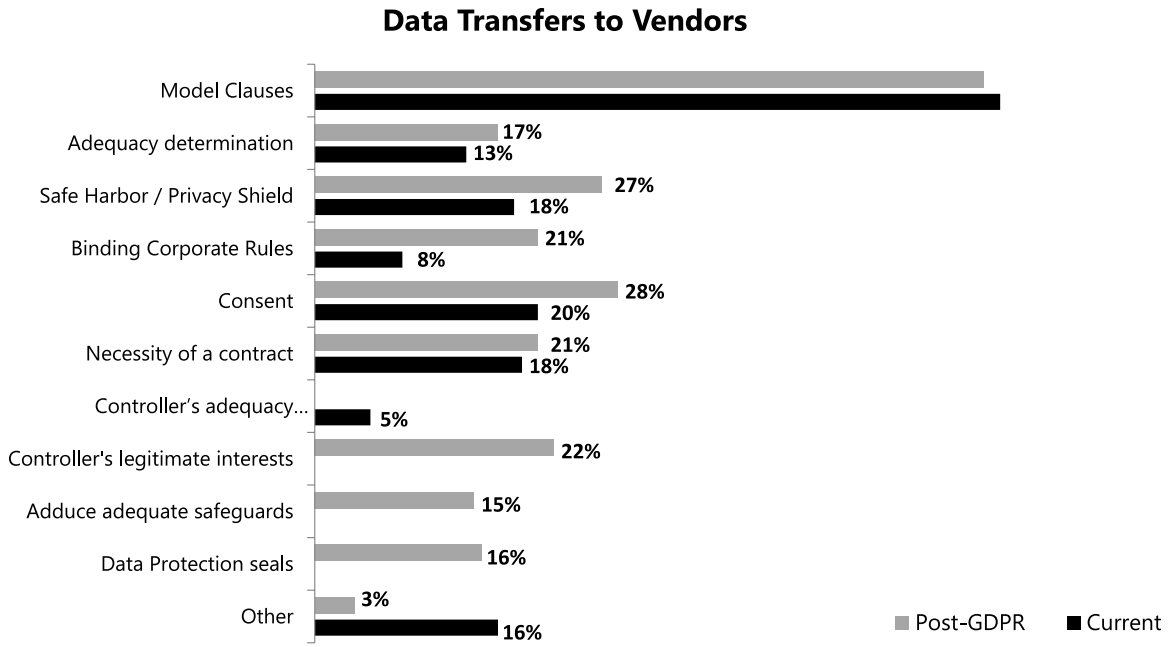
e) Post-GDPR, organisations will rely less on consent of individuals as a basis for transfers of HR and consumer/customer data.

f) Survey respondents also intend to use new data transfer mechanisms created by the GDPR. In particular, 10-15 percent intend to use ad hoc, adequate safeguards, and 10-16 percent intend to use data protection seals and certifications. This shows that there is commercial appetite for such mechanisms, despite there not being much detail or information on how these will work in practice and the level of the DPAs' involvement or approval process.

Indicate the current data transfer mechanisms you rely upon and you intend to use once the GDPR enters into force







7. Breach notification

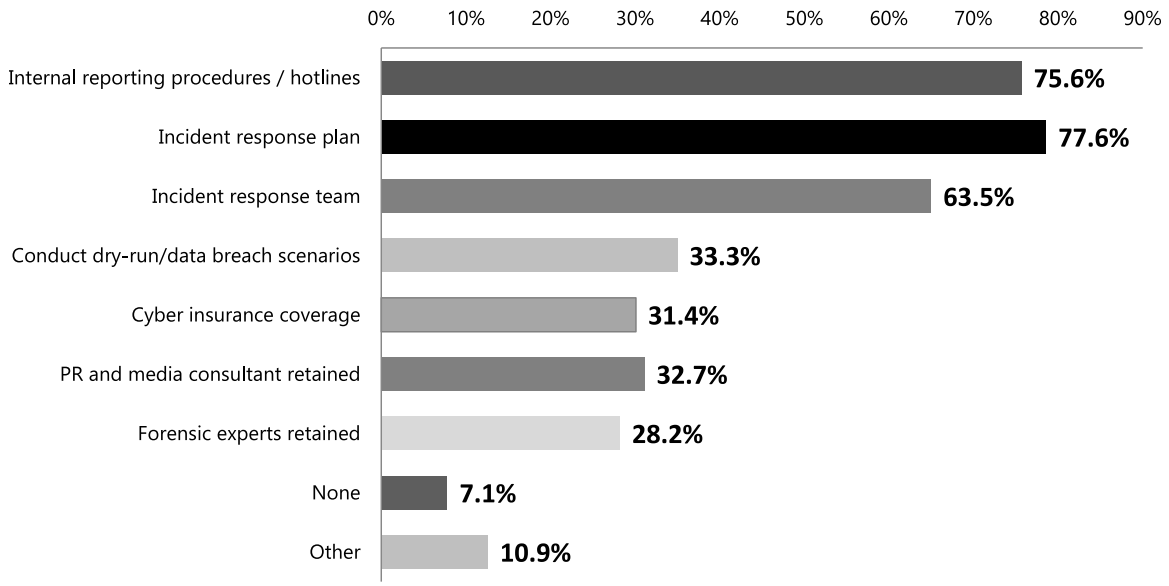
One of the key changes under the GDPR is the data breach notification obligation. A controller will have to notify the DPA within 72 hours after becoming aware of any breach that presents risks to the rights and freedoms of individuals. If such a breach presents a high risk to the rights and freedoms of the individuals, the controller will also have to notify each of the affected individuals without undue delay. Processors will also have to notify controllers without undue delay after becoming aware of a breach.

The survey results show that the majority of survey respondents are well prepared for the breach notification obligations. More than 75 percent have internal reporting procedures, 78 percent have an incident response plan, and 64 percent have an incident response team. Such results are not surprising, given that 77 percent of respondents are already subject to data breach reporting obligations, either voluntary or mandatory, under other laws, including the ePrivacy Directive, US breach notification laws, and other EU and non-EU national laws.

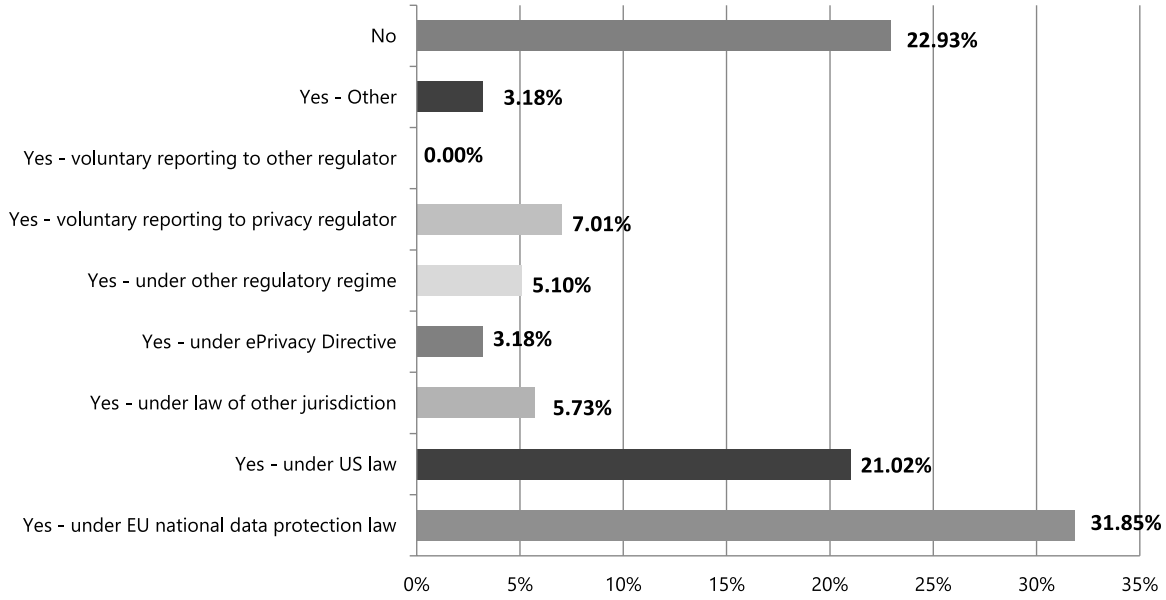
That said, less than a third of organisations appear to have implemented other best practice measures and procedures, such as conducting "dry runs" to practice response to breach scenarios, procuring cyber insurance, or retaining PR and media consultants – with only 28 percent currently engaging forensic experts.

This is perhaps not surprising and shows that the breach reporting landscape (and associated industry) is very much in its infancy in the EU. These are areas where all organisations will have to step up their GDPR implementation measures in light of increased cybersecurity needs and other threats.

What measures and procedures do you currently have in place to respond to data breaches?

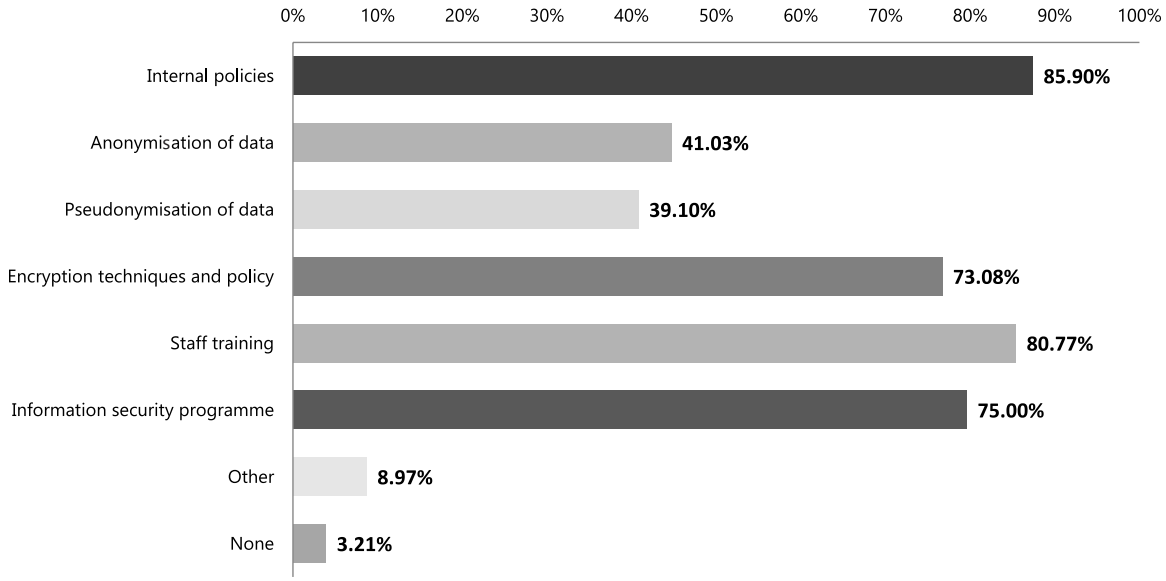


Is your organisation currently subject to a data breach reporting obligation, or does your organisation voluntarily report data breaches?



In addition to putting in place procedures to deal with breaches, it is encouraging to see that the majority of organisations are also proactively implementing organisational and technical measures to minimise the likelihood and impact of a breach. The majority of respondents are implementing internal policies (86 percent), staff training (81 percent) or information security programmes (75 percent), as well as encryption techniques (73 percent).

What security measures does your organisation implement to minimise the likelihood and impact of a data breach?

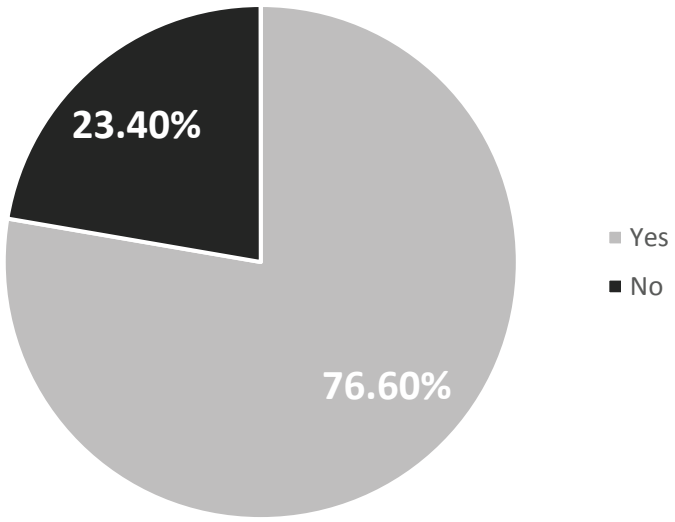


8. Main establishment

Under the GDPR, a controller or processor may elect a lead supervisory authority based on the main establishment for its processing activities. Survey respondents were largely confident (77 percent) in their ability to determine their main establishment and lead supervisory authority once the GDPR enters into force.

This seems to reflect the positive reaction to the concept of the one-stop shop. However, it may overlook some of the complexities that arise for companies when considering the criteria for determining where their main establishment is. For instance, based on the criteria there could be one main establishment for one type of personal data (such as HR data) and a different establishment for another type of data (such as customer data).

Are you able to determine your main establishment and lead supervisory authority once the GDPR enters into force?



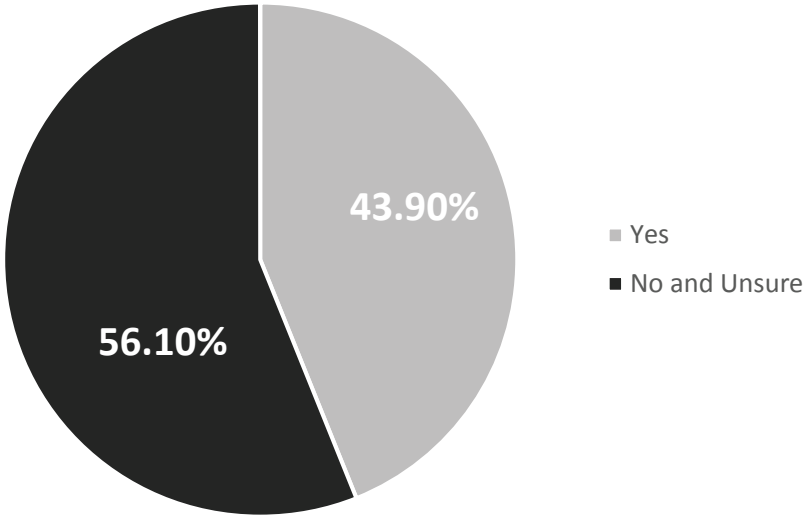
9. Data portability

The GDPR introduces a new right of data portability for individuals. This means that individuals have the right to obtain their personal data in a machine readable format request that the data is transferred directly from one controller to another.

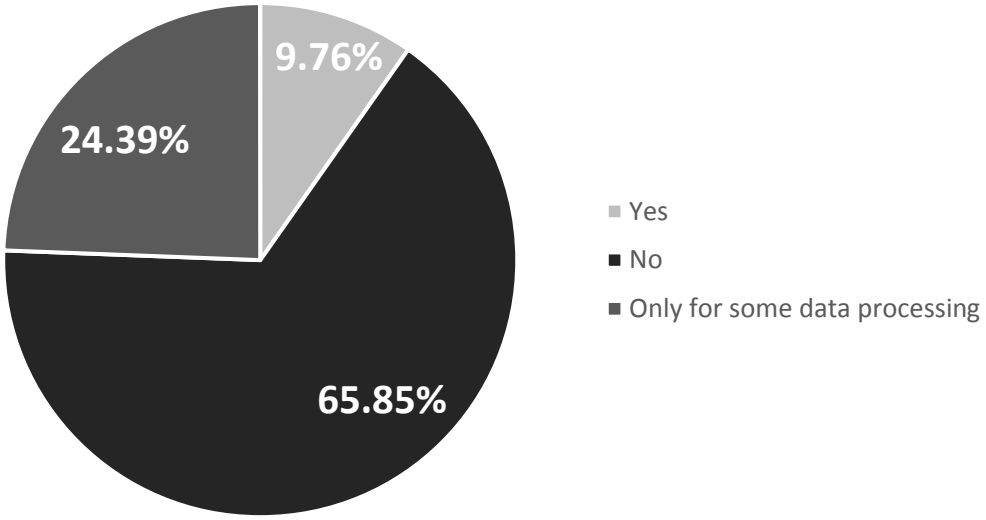
The survey results show some confusion around the application of the right to data portability, with the majority of respondents saying it doesn't apply to their organisation, or that they are unsure (56 percent). Further, it appears that two thirds of survey respondents (66 percent) do not currently have procedures

in places to enable an individual to transmit his or her personal data to another controller in a machine readable format. This is not surprising given the fact that this is a new right, stemming from consumer protection, and with limited existing experience. It will take time for organisations to understand and assess the full impact of this new right and build procedures and technical measures for proper execution of data portability requests in respect to all different legacy and new customer data systems.

Do you consider the right to data portability to be relevant for your data processing?



Do you have procedures to enable an individual to transmit his or her personal data to another controller in a machine readable format?



10. Data processing inventory

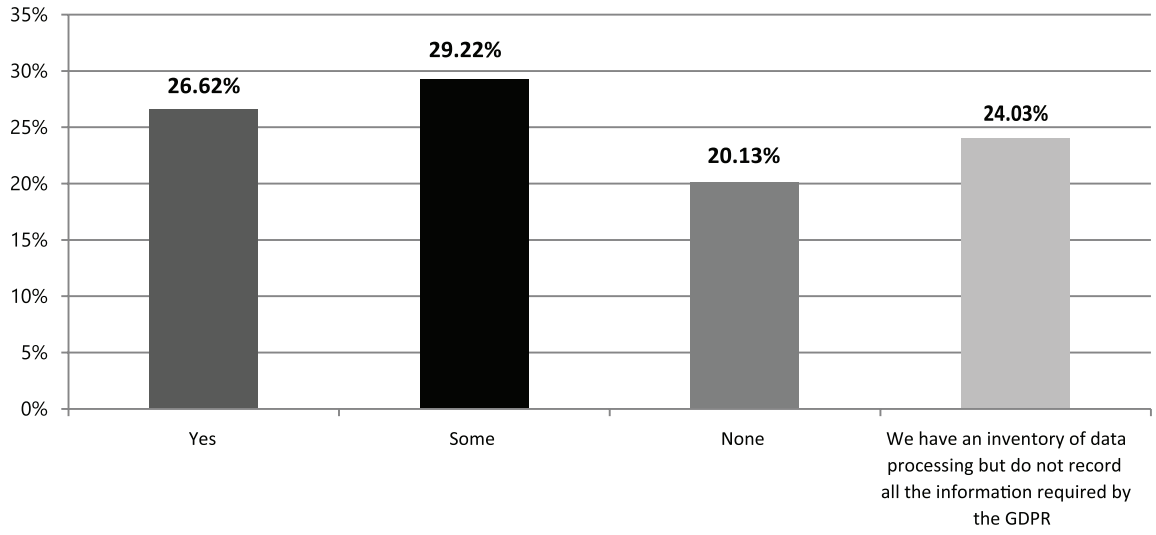
The GDPR replaces the current obligation of the Directive to register processing activities and systems DPAs with the requirement to keep internal records of all data processing activities. The new requirement applies to both controllers and processors.

According to respondents, 27 percent have an up to date record/register/inventory of the personal data they hold, including the purposes for which data is used and other information as required by the GDPR. Another 29 percent state that they hold some of this information.

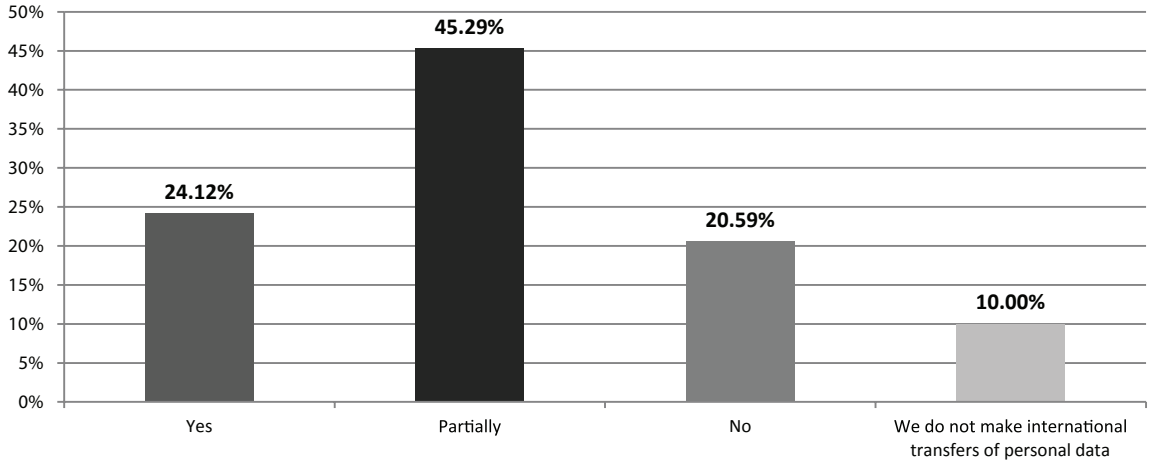
On the other hand, one fifth of organisations do not have any internal records in place and just under a quarter hold some records, but not to the level required by the GDPR. Clearly this will be an area where many organisations will have to step up their implementation efforts and seek tools and software to help them comply with this obligation.

Data inventories and records appear to be more present in respect of data transfers, with almost 70 percent of respondents having the relevant information in relation to their data transfers (either all the information or some of it).

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



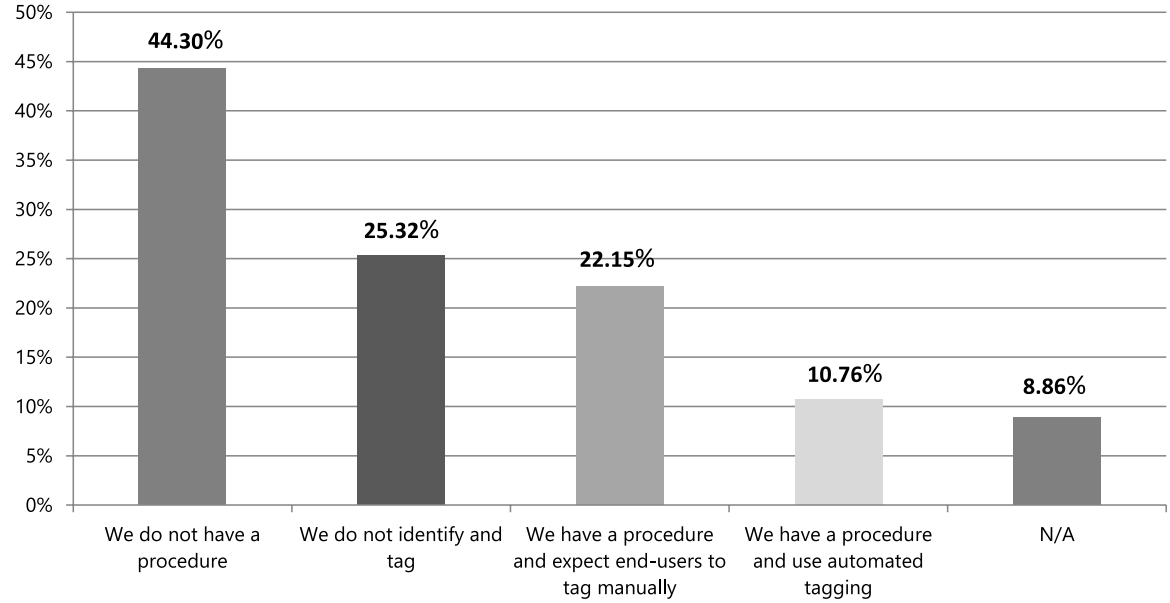
Do you hold a record/inventory of the international transfers of personal data made by your organisation?



10.1 Data tagging and classification

Closely related to data processing inventories is data tagging and classification practices. The survey shows that only one third of organisations regularly tag and classify data that they hold to determine whether or not this data contains personal or sensitive information. In addition, only 10 percent use any kind of automation for this process. The others rely on end users to tag data manually.

This is likely going to be one area where organisations will need to invest in technology and processes that automate and industrialise data tagging and classification, rather than leaving it to end users to tag their own data and implement the company's policies. Again, this will be an area that will require close cooperation between the DPO. CISO, IT, and CIO functions in an organisation.

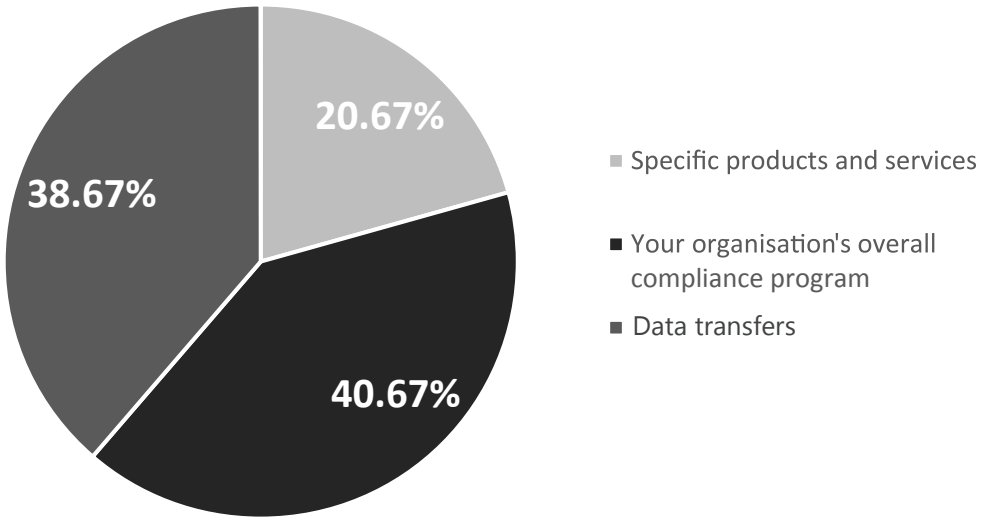


11. Seals and certification

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. DPAs and third-party-certifying bodies will be able to issue the seals and certifications to organisations that wish to apply.

Survey respondents appear to be interested in the use of data protection seals and certifications. Interestingly, 41 percent view a seal or certification as being able to demonstrate their organisation's overall data privacy compliance programme. Another significant number of respondents see them more in the context of specific products or services (39 percent), followed by 21 percent who see them as a useful tool for legitimising data transfers.

Please select any of the following from the list below if you would consider relying on data protection seals or certifications. Specific products and services, your organisation's overall compliance programme or data transfers.



Glossary of Key GDPR Terms

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.

Centre for Information Policy Leadership
Hunton & Williams LLP

A GLOBAL PRIVACY AND SECURITY THINK TANK

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

ACTIVE GLOBAL REACH

45+
Member companies

5+
Active projects & initiatives

20+
Conferences, workshops & events annually

15+
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, regulators and policy makers to develop global solutions and best practices for privacy and responsible use of data to enable the modern information age.

Bojana Bellamy
President
bbellamy@hunton.com

Markus Heyder
Vice President & Senior Policy Counselor
mheyder@hunton.com

Michelle Marcoot
Director, Business Development
mmarcoot@hunton.com

twitter.com/the_cipl

linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Avenue
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

AvePoint®

AvePoint at a Glance

Founded in 2001, AvePoint helps more than 15,000 organizations accelerate the migration, management, and protection of their data no matter where it lives – including IT systems on premises, in the cloud, and in hybrid environments.

Migration

Management

Protection

AvePoint, Inc. is headquartered and maintains its principal operational center in Jersey City, NJ, with approximately 1,600 employees located in wholly owned operational centers on five continents.

- Australia
- Canada
- China
- France
- Germany
- Japan
- Netherlands
- Singapore
- South Africa
- Sweden
- Switzerland
- United Kingdom
- Chicago, IL (US)
- Irving, TX (US)
- Seattle, WA (US)

iapp PLATINUM MEMBER

Customers

88
Countries

6
Continents

Deloitte
Technology Fast 500

Inc. Magazine
Hire Power Award
Inc. 500|5000

Ernst & Young
Entrepreneur of the Year

Windows IT Pro
Best SharePoint Product

Global, Live Support 24/7

SharePoint · Office 365 · yammer · box · File Systems · Databases · Websites