

BAKER & MCKENZIE



# PREPARING FOR NEW PRIVACY REGIMES:

PRIVACY PROFESSIONALS' VIEWS  
ON THE GENERAL DATA PROTECTION  
REGULATION AND PRIVACY SHIELD

# EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) and proposed EU-U.S. Privacy Shield are the results of a concerted effort to strengthen data privacy and protection for individuals within the EU. To explore privacy professionals' views, expectations and concerns in regards to these regimes, Baker & McKenzie deployed a survey during the International Association of Privacy Professionals' (IAPP) Global Privacy Summit from April 4-6, 2016 in Washington, DC. The IAPP Global Privacy Summit is widely seen as one of the largest privacy law conferences in the world.

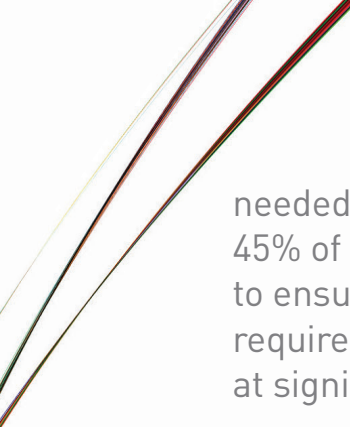
---

**Privacy professionals appear to agree that the GDPR and Privacy Shield represent a call-to-action for organizations generally.**

---

110 individuals responded to the survey and Baker & McKenzie is pleased to offer this report summarizing the themes and insights arising from their feedback. One of the key takeaways from the survey results is the consensus among privacy professionals that the GDPR and Privacy Shield represent a call-to-action for organizations generally. The majority of respondents believe that the GDPR will impact their organization and will require organizations to invest at least some, if not significantly, more budget and effort to comply. Similarly, most respondents indicated that organizations should self-certify to the Privacy Shield once it is validated and implement data transfer agreements in the interim.

Regarding specific requirements under the GDPR, its consent, data mapping and cross-border transfer requirements were identified as being among the most difficult to comply with—around 70% of respondents indicated that at least some additional budget/effort is



needed to comply with these requirements. In addition, around 45% of respondents indicated that they either do not have the tools to ensure that their organization complies with the main requirements under the GDPR, or else could only obtain such tools at significant cost.

Regarding the Privacy Shield Program, which is a proposed agreement between the EU and U.S. to allow certain transfers of personal data between the two jurisdictions, the majority of respondents recommend that organizations self-certify to the program within two months of the regime's effective date. An organization that does so will, under the current draft of the

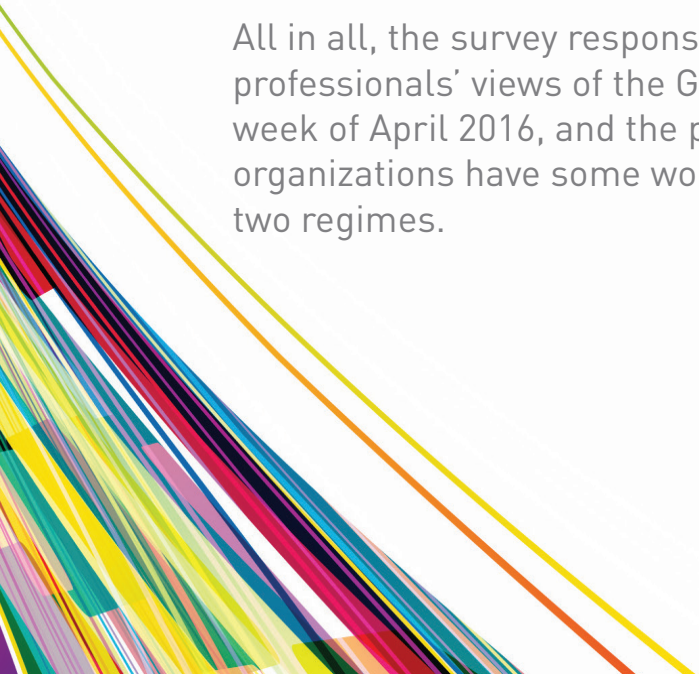
---

**The majority of respondents believe that organizations would generally benefit from taking advantage of the two-month transition period under the Privacy Shield with respect to third-party contractual relationships.**

---

framework, have up to nine months from the date upon which it self-certifies to bring its third-party contractual relationships in line with the Privacy Shield principles. Most privacy professionals also believe that implementing data transfer agreements and/or binding corporate rules in addition to self-certifying to Privacy Shield would strengthen the protection for cross-border data transfers.

All in all, the survey responses provide a snapshot of privacy professionals' views of the GDPR and Privacy Shield during the first week of April 2016, and the picture that emerges suggests that organizations have some work ahead of them in preparation of the two regimes.



# SURVEY RESPONDENTS

Over 100 privacy professionals participated in the survey in total. The respondents mostly included senior managers and individuals involved in data privacy and security, including privacy and security officers, privacy regulators, compliance managers, privacy attorneys and consultants, data strategy managers, IT personnel, and privacy analysts and students.

More than 70% of respondents self-identified as being members of a multinational organization, with the remainder largely being associated with government agencies, regulatory bodies, or policy and academic institutions.



# EU General Data Protection Regulation (GDPR)

## Familiarity with the GDPR

Over 80% of respondents noted that they are at least somewhat familiar with all of the major requirements under the GDPR. The figure below illustrates respondents' familiarity with each of the listed types of requirements and provisions under the GDPR.

How familiar are you with the following GDPR requirements?

GDPR Requirements	Not familiar	Somewhat familiar	Familiar	Very familiar
Consent requirements	10%	38%	36%	17%
Data breach reporting obligations	11%	30%	44%	15%
DPO requirements	14%	30%	41%	15%
Data mapping requirements	15%	38%	36%	12%
Data subject rights (e.g., access & portability)	11%	34%	42%	13%
Privacy by design requirements	13%	32%	39%	16%
Profiling restrictions	16%	41%	33%	10%
Cross-border data transfer requirements	11%	29%	37%	24%
Accountability requirements	11%	31%	46%	19%
Privacy impact assessment requirements	13%	28%	40%	19%
Information security requirements	13%	30%	32%	25%
Data processor obligations	10%	33%	40%	17%
Employee privacy training requirements	13%	30%	37%	20%
Potential enforcement actions and sanctions for noncompliance	12%	27%	42%	19%

All percentages in this report have been rounded to the nearest percent.

The fact that so many survey respondents are familiar with the requirements of the GDPR more than two years before its effective date speaks to the importance of the GDPR and its anticipated impact. These results also lend greater credence to the remaining GDPR-related responses.

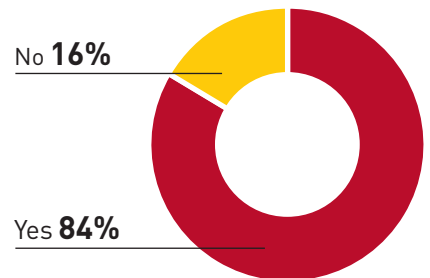
At the same time, these results indicate that **privacy professionals are least familiar with the data mapping requirements and profiling restrictions under the GDPR.** Given that these requirements, among others, do not have direct analogues in the GDPR's predecessor, it is not surprising that privacy professionals would need to engage in further efforts to familiarize themselves with such requirements. For more information on some of the main requirements under the GDPR, please see Baker & McKenzie's [GDPR Game Plan](#).

## Anticipated Impact of the GDPR

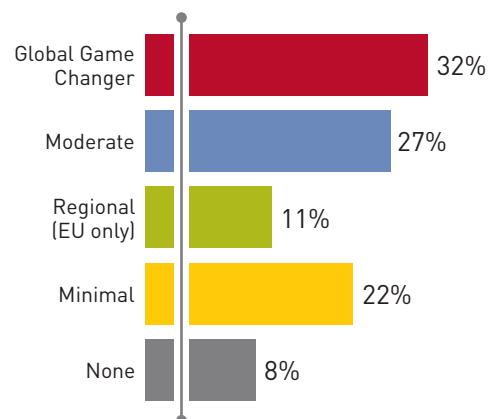
**The vast majority of respondents (84%) indicated that they anticipate that the GDPR will impact their organization.**

Asked to gauge the anticipated level of impact that the GDPR will have on their organization, **roughly a third of respondents agreed that the GDPR represents a Global Game-Changer.** Over a third of respondents indicated that they believe that the GDPR's impact will be moderate or focused on the EU only, with the remainder positing that the GDPR will have a minimal or no impact on their organizations.

Do you anticipate that the GDPR will impact your organization?



What level of impact do you foresee that the GDPR will have on your organization?



## Anticipated Budget and Effort Needed to Comply with GDPR

The majority of respondents believe that organizations will need to invest additional budget and effort to comply with the GDPR. The chart below summarizes the level of budget/effort respondents foresee organizations will need to invest to comply with the major requirements under the GDPR.

How difficult do you think it will be for organizations to comply with the following GDPR requirements?

GDPR Requirements	Significantly more budget/effort needed to comply	Some additional budget/effort needed to comply	Existing compliance efforts will be sufficient	GDPR is less stringent than the status quo	I don't know
Consent requirements	19%	51%	15%	2%	13%
Data breach reporting obligations	18%	48%	15%	3%	15%
DPO (data privacy/protection officer) requirements	22%	41%	20%	2%	15%
Data mapping requirements	14%	56%	12%	1%	17%
Data subject rights	13%	51%	17%	1%	18%
Privacy by design requirements	16%	47%	18%	1%	17%
Profiling restrictions	16%	50%	13%	1%	20%
Cross-border data transfer requirements	13%	55%	16%	2%	14%
Accountability requirements	24%	41%	13%	3%	19%
Privacy impact assessment requirements	17%	47%	15%	2%	18%
Information security requirements	14%	51%	16%	3%	16%
Data processor obligations	16%	48%	15%	2%	18%
Employee privacy training requirements	14%	52%	14%	1%	19%

In general, around 60-70% of respondents believe that organizations will need to spend at least some, if not significantly, more budget and effort to comply with the GDPR. In particular, **around 70% of respondents believe that organizations will need to invest additional budget/effort to comply with the consent, data mapping and cross-border data transfer requirements under the GDPR.**

The requirements most frequently flagged as requiring *significantly* more budget and effort for compliance were the accountability, data privacy/protection officer and consent requirements under the GDPR. Conversely, the most number of respondents indicated that their existing compliance efforts would be sufficient to comply with the GDPR's data privacy/protection officer (DPO) and privacy by design requirements.





## Availability of GDPR Compliance Tools

On average, around 45% of respondents indicated that they either do not have the tools to ensure that their organization complies with the main requirements under the GDPR, or else could only obtain such tools at significant cost. The figure below illustrates respondents' familiarity with each of the listed types of requirements and provisions under the GDPR.

Do you have the tools to ensure that your organization complies with the following GDPR?

GDPR Requirements	Yes	Possibly, but at significant cost	No
Consent requirements	58%	27%	15%
Data breach reporting obligations	55%	29%	16%
DPO (data privacy/protection officer) requirements	60%	22%	18%
Data mapping requirements	44%	40%	16%
Data subject rights	50%	32%	18%
Privacy by design requirements	46%	36%	18%
Profiling restrictions	50%	27%	24%
Cross-border data transfer requirements	63%	23%	14%
Accountability requirements	55%	34%	11%
Privacy impact assessment requirements	53%	32%	15%
Information security requirements	62%	27%	11%
Data processor obligations	54%	30%	16%
Employee privacy training requirements	58%	29%	13%

The least number of survey respondents appear to have easy access to tools to ensure compliance with the requirements regarding data mapping, privacy by design and profiling restrictions. Conversely, the most number of respondents answered that they can easily access the tools to ensure that their organization complies with the data privacy/protection officer, cross-border transfer and information security requirements.





## Summary of GDPR Feedback

The survey responses provide a valuable snapshot of privacy professionals' views on the GDPR just prior to the EU Parliament's formal adoption of the regulation on April 14, 2016. Probably the key takeaway is that privacy professionals seem largely to agree that the GDPR will have a material impact on their organization and that their organization will need to invest additional budget, time and effort to ensuring that it complies with the GDPR.

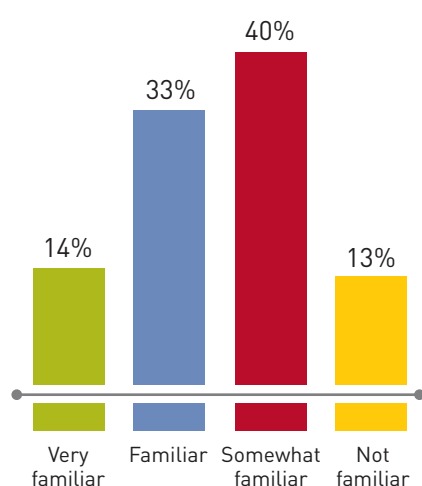
Given the severe penalties of up to EUR 20 million or 4% of total global annual turnover in fines for non-compliance under the GDPR, organizations would be well-advised to begin taking steps to ensure that they understand and comply with the requirements under the GDPR prior to its anticipated effective date in 2018. Baker & McKenzie regularly posts updates regarding the GDPR on its free online magazine [b:INFORM](#), and interested users should subscribe through the website to receive the b:INFORM newsletter. In addition, Baker & McKenzie has prepared the free [GDPR Game Plan](#) to assist organizations in complying with the GDPR.



# EU-U.S. Privacy Shield

## Familiarity with Privacy Shield

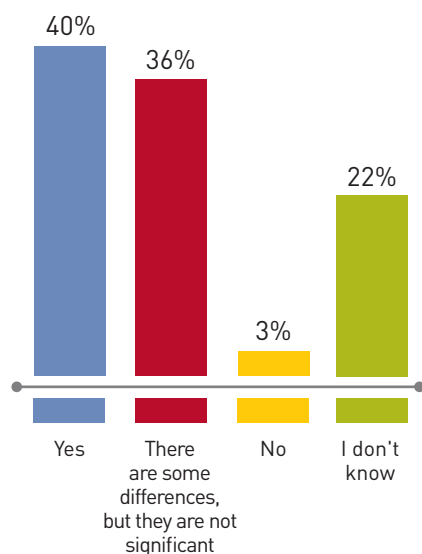
How familiar are you with the EU-US Privacy Shield?



Over 85% of survey respondents indicated that they are at least somewhat familiar with the Privacy Shield, with around half of respondents indicating that they are familiar or very familiar with the regime.

As with the GDPR, the survey respondents' strong familiarity with the requirements of the proposed successor to the EU-U.S. Safe Harbor Program is indicative of the significance of the Privacy Shield and its anticipated impact. These results also lend greater credence to the remaining Privacy Shield-related responses.

Do you think there are significant differences between the EU-US Safe Harbor agreement and the EU-US Privacy Shield?



## Privacy Shield vs. Safe Harbor

Approximately three-quarters of survey respondents find that there are differences between Safe Harbor and Privacy Shield, although only 40% of survey respondents believe such differences are significant.

For more information on some of the new requirements introduced under the proposed Privacy Shield Program, please see our [b:INFORM commentary](#), and stay tuned for additional Baker & McKenzie commentary in the wake of the Article 29 Working Party's published opinions on the adequacy of the framework.

# Protecting Cross-Border Data Transfers

Asked to identify which cross-border data transfer mechanisms they consider to adequately safeguard data subjects' personal information/data and rights, **the majority of respondents opined that data transfer agreements (59%), model contract clauses approved by a relevant authority such as the EU Commission (56%) and binding corporate rules approved by privacy authorities in the EEA (57%) offer adequate protection.**

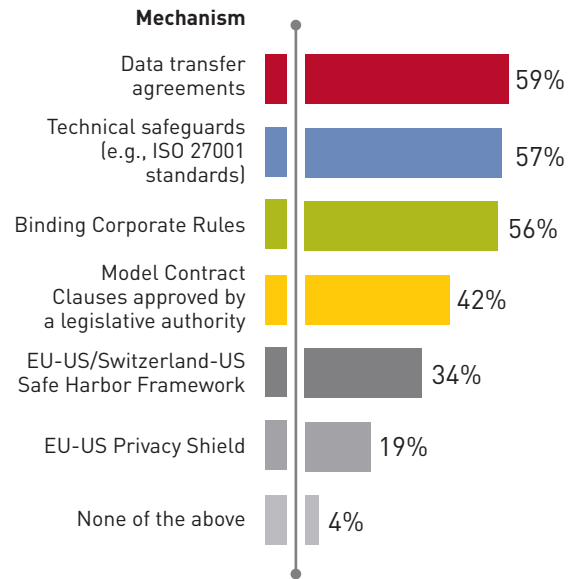
Only 42% of respondents selected Privacy Shield as an adequate cross-border data transfer mechanism, which was nonetheless more than double the number of respondents who selected the EU-U.S. Safe Harbor Framework (19%).

## Advisability of Self-Certification to Privacy Shield

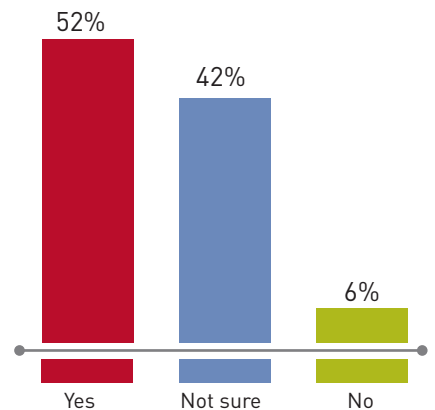
**The majority of privacy professionals who responded to the survey recommend that organizations sign up to the program (52%), although a significant portion of respondents expressed that they were not sure (42%).**

It is noteworthy that a majority of respondents indicated that they would recommend that organizations should self-certify to the Privacy Shield, as it suggests that Privacy Shield will have a strong participation and following.

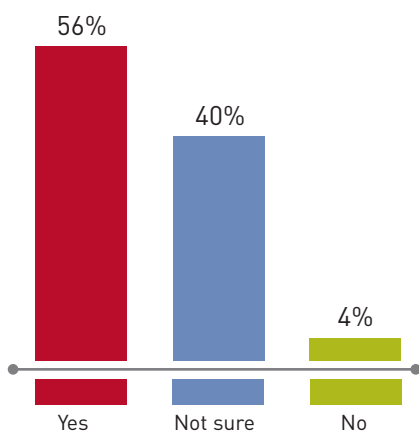
Which of the following cross-border data transfer mechanisms do you consider to adequately safeguard data subjects' personal information/data and rights? (check all that apply)



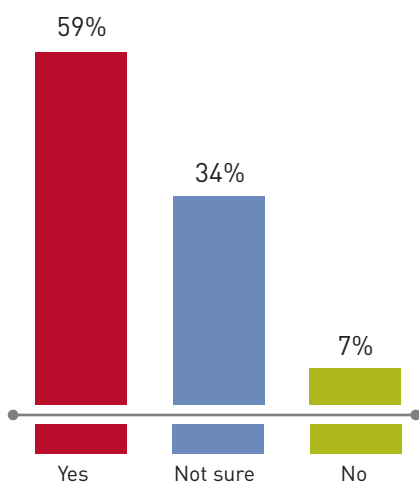
Would you recommend that organizations sign up to the Privacy Shield?



Do you believe that organizations would generally benefit from taking advantage of the two-month transition period with respect to third-party contractual relationships?



In the interim before the Privacy Shield is validated, should organizations implement data transfer agreements?



The majority of respondents also believe that organizations would generally benefit from taking advantage of the two-month transition period under the Privacy Shield with respect to third-party contractual relationships. Specifically, draft Privacy Shield provides that if an organization certifies to the Privacy Shield within two months of the framework's effective date, the organization will have up to nine months from the date upon which it certifies to bring such relationships with third parties in line with the Accountability for Onward Transfer Principle. This information was made known to respondents prior to them answering this question.

## Prior to Validation of Privacy Shield

Almost 60% of respondents believe that organizations should implement data transfer agreements in the interim before Privacy Shield is validated, although roughly one-third of respondents were not sure whether organizations should do so.





## Summary of Privacy Shield Feedback

The survey responses illustrate that the majority of privacy professionals would appear to recommend that organizations self-certify to the Privacy Shield Program within two months after it has been validated. With the publication of the Article 29 Working Party's opinion on April 13, 2016 that the current draft of the Privacy Shield Principles is inadequate, it may be some time yet before the Privacy Shield Program is implemented. In the meantime, most privacy professionals seem to agree that an organization ought to implement data transfer agreements to legitimize their transatlantic personal data flows.

Baker & McKenzie regularly posts updates regarding the Privacy Shield on its free online magazine [b:INFORM](#), and interested users should subscribe through the website to receive the b:INFORM newsletter.



## Baker & McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in more than 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.