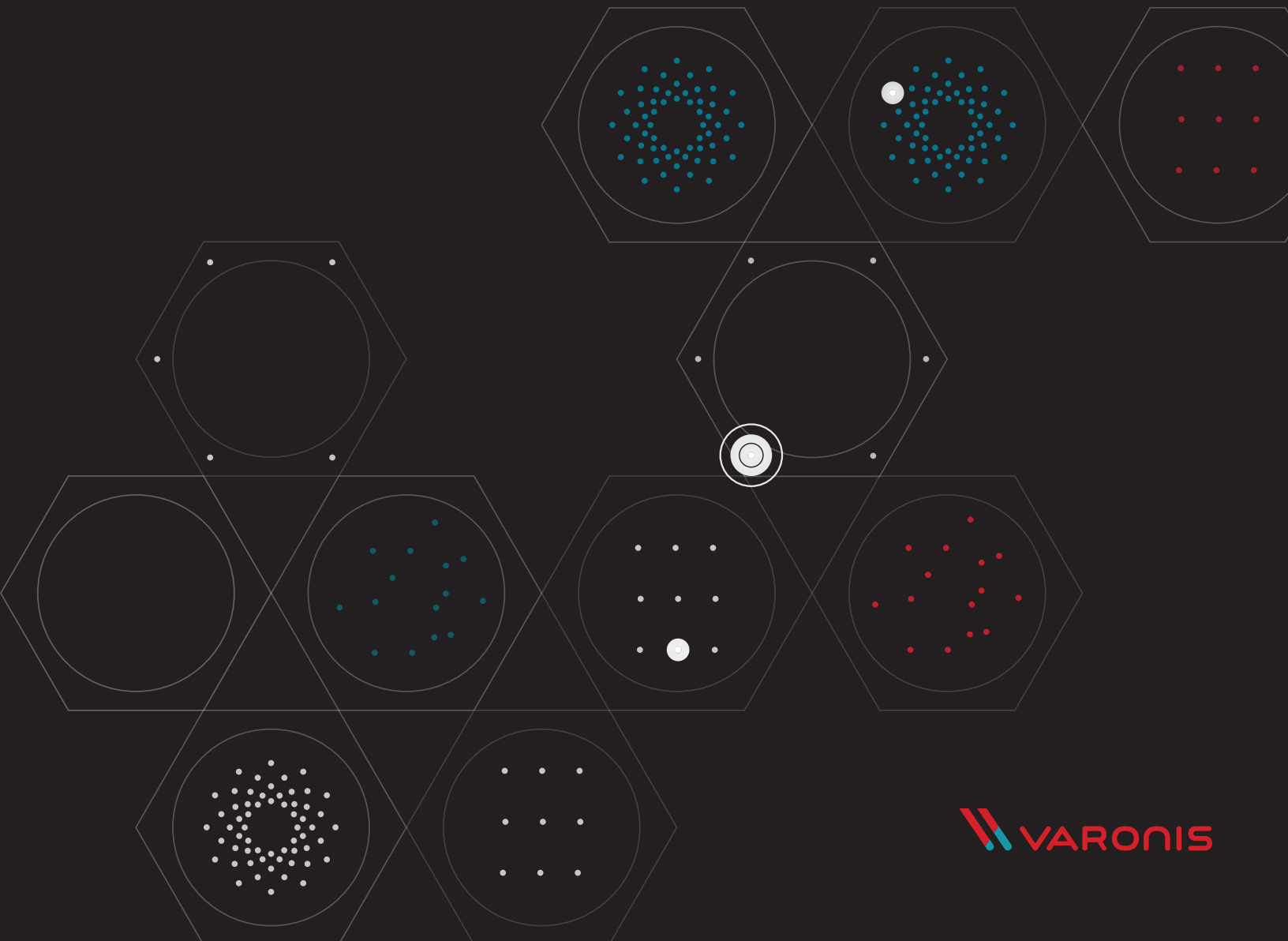# Countdown to GDPR:

Challenges and Concerns

With just months left to go before the General Data Protection Regulation (GDPR) deadline on May 25, 2018, we wanted to understand where cybersecurity professionals stand in their preparations and attitudes toward this landmark regulation.

KEY FINDINGS

- 60% of respondents in the EU and 50% of respondents in the U.S. say they face some serious challenges in being GDPR compliant.

- Organizations are making progress on GDPR: 35% in Germany, 42% in France, and 36% in the UK report being in compliance. In the EU, almost half of respondents say their organization is more than 50% complete in their compliance process.

- About two in five respondents feel their organizations have not yet completed their evaluation of procedures and assessment for existence of personal information. Other measures have been completed by, at most, half of respondent organizations.

- Respondents considered the greatest GDPR challenge to be Article 17 (the right to erasure/'to be forgotten'), followed by Article 25 (data protection by design). Among all respondents, the greatest concern centers around the potential for crippling fines for breaches.

- By far, data security is considered to be the most important aspect in ensuring compliance with GDPR. Network security is second, and application security last.

- Nearly nine in 10 of those in the EU are aware of GDPR, compared to only two in three in the US. One in four U.S. respondents believe their firms need not comply with GDPR.

ABOUT THE SURVEY

This independent survey on top concerns, approaches
and experiences of cybersecurity professionals regarding
the GDPR was commissioned by Varonis and carried out by
Survey Sampling International.

- ⬣ 500 surveyed: 200 in the U.S., 100 each in the UK, France and Germany

- ⬣ All respondents are involved in IT and are personally responsible for cybersecurity

- ⬣ Respondents are from organizations with more than 1,000 employees

- ⬣ All respondents work for organizations that collect, generate or possess sensitive data such as PII and payment card information

- ⬣ The survey was conducted between September 28 – October 6, 2017

When GDPR goes into effect, organizations that store, process or share EU citizens' personal data must follow the rules. The rules apply to organizations that promote goods or services in the EU, regardless of location.
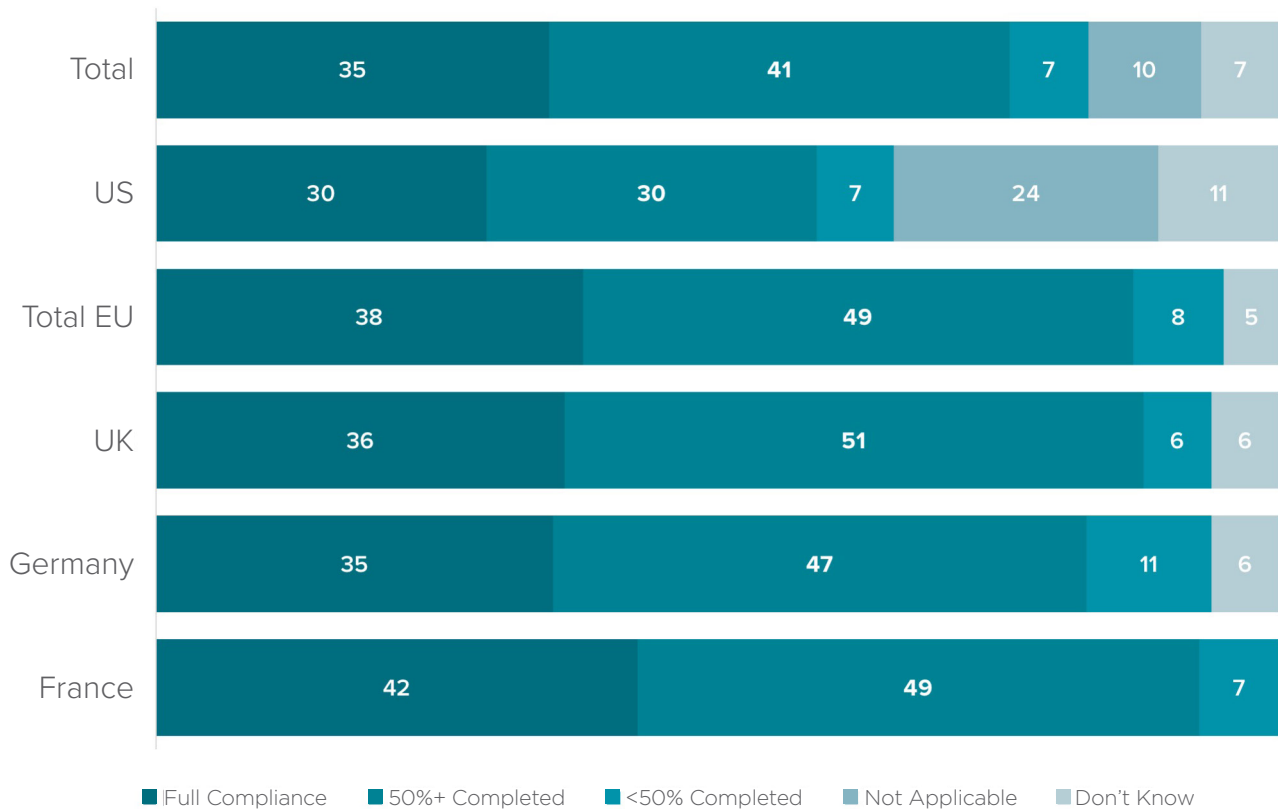
While most respondents in the EU (88%) are aware of GDPR, respondents in the U.S. are less familiar (65%).
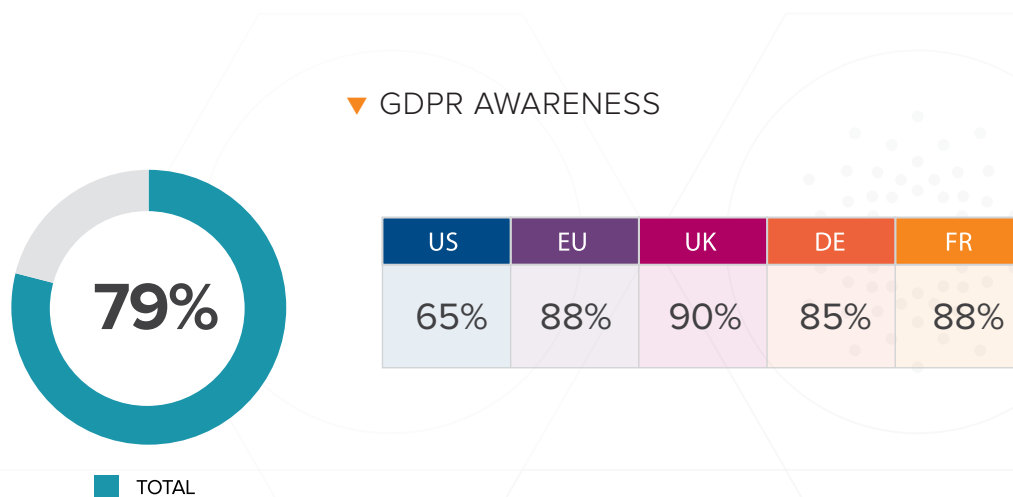
▼ GDPR AWARENESS

79%

US	EU	UK	DE	FR
65%	88%	90%	85%	88%

■ TOTAL

Organizations are taking GDPR seriously: Over a third (38%) of respondents surveyed in France, Germany and the UK are currently in compliance with GDPR. In the EU, 49% of respondents say their organization is more than 50% complete in their compliance process. One in four U.S. respondents believe their firms do not need to comply with GDPR.

▼ COMPLIANCE WITH GDPR

Region	Full Compliance	50%+ Completed	<50% Completed	Not Applicable	Don't Know
Total	35	41	7	10	7
US	30	30	7	24	11
Total EU	38	49		8	5
UK	36	51		6	6
Germany	35	47		11	6
France	42	49	7		

■ Full Compliance　■ 50%+ Completed　■ <50% Completed　■ Not Applicable　■ Don't Know

* Percentages have been rounded to the nearest whole number

Which of the following security measures has your organization already completed to get into compliance with GDPR?
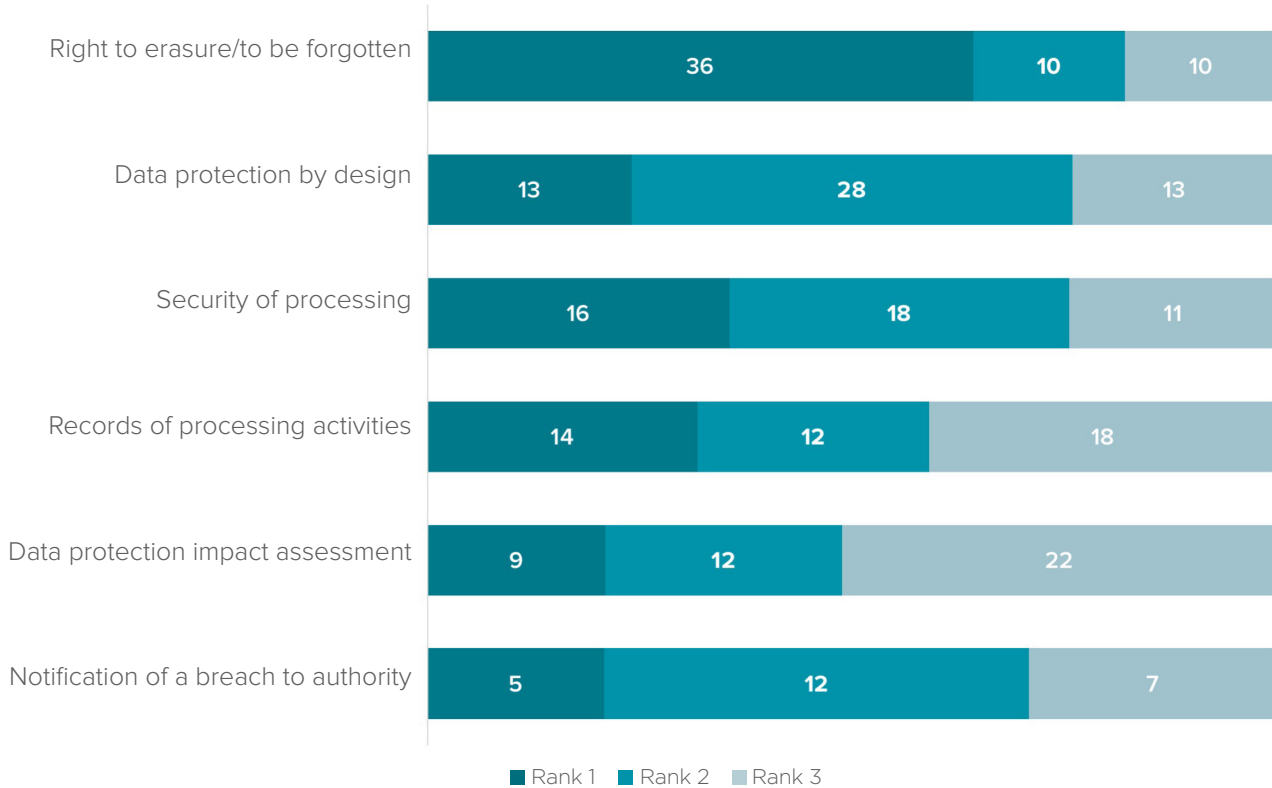
Much work is left to do in preparation for GDPR. About two in five respondents feel their organizations have not yet completed their evaluation of procedures and assessment for existence of personal information. Other measures have been completed by half or fewer of respondent organizations.

▼ MEASURES COMPLETED

	US	EU	UK	DE	FR
Educating employees of the changes around GDPR	46%	48%	52%	43%	49%
Hiring a data protection officer (DPO)	22%	37%	34%	53%	25%
Hiring a chief digital officer (CDO)	22%	29%	26%	35%	25%
Hiring a chief privacy officer (CPO)	24%	18%	18%	19%	16%
Re-evaluating procedures for detecting, reporting and investigating a breach	67%	60%	66%	46%	69%
Assessing what personal information you have across your organization	59%	62%	65%	69%	53%
Adopting privacy-by-design (meaning that each new service or business process that makes use of personal data must take the protection of such data into consideration)	50%	51%	42%	48%	62%
Other	0%	1%	2%	0%	0%
None of the above	7%	3%	6%	1%	2%

Which of the following rules do you believe are going to represent the greatest challenge to your organization with regard to meeting the GDPR?

Respondents were asked to select and rank their top three concerns related to GDPR. Article 17 (right to erasure/to be forgotten) is the greatest challenge in meeting GDPR, according to survey respondents. Article 25 (data protection by design) ranked second and Article 32 (security of processing) third.

	Rank 1	Rank 2	Rank 3
Right to erasure/to be forgotten	36	10	10
Data protection by design	13	28	13
Security of processing	16	18	11
Records of processing activities	14	12	18
Data protection impact assessment	9	12	22
Notification of a breach to authority	5	12	7

■ Rank 1   ■ Rank 2   ■ Rank 3

▼ TOP THREE CHALLENGES (RANKED 1ST, 2ND OR 3RD)

US	TOTAL EU	UK	GERMANY	FRANCE
52% Security of processing	**58%** Right to erasure	**58%** Data protection by design	**62%** Right to erasure	**64%** Right to erasure
48% Data protection by design	**57%** Data protection by design	**51%** Right to erasure	**50%** Data protection by design	**64%** Data protection by design
48% Records of activities	**42%** Security of processing	**49%** Records of activities	**47%** Records of activities	**43%** Impact assessment
	42% Records of activities			

To what extent do you agree or disagree: We face some serious challenges in being compliant with the EU GDPR by 25 May 2018

Overall, organizations do not seem to be moving as fast as they need to on GDPR. In fact, 60% of respondents in the EU and 50% of respondents in the U.S. say they face some serious challenges in being compliant by the May deadline.

We face some serious challenges in being compliant	17	40	29	8	6

■ Agree Strongly   ■ Agree   ■ Disagree   ■ Disagree Strongly   ■ Don't Know
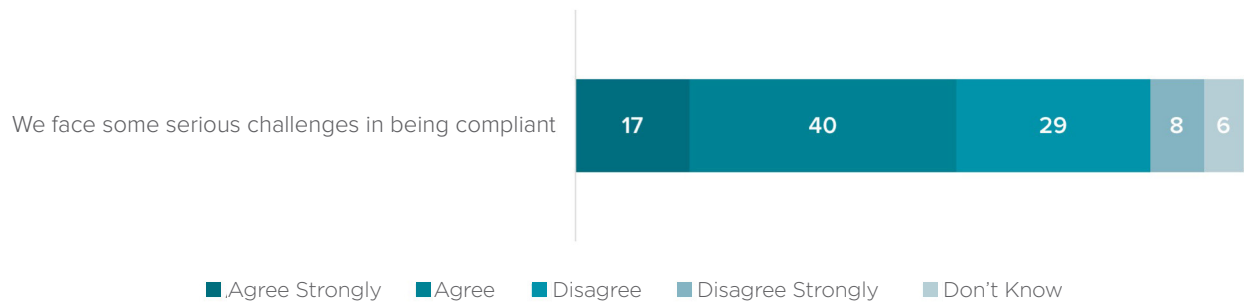
▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Strongly Agree/Agree (Net)	50%	60%	61%	71%	48%
Strongly Agree	17%	16%	16%	20%	13%
Agree	33%	44%	45%	51%	35%
Disagree	30%	29%	29%	22%	35%
Strongly Disagree	11%	7%	2%	4%	14%
Don't Know	9%	4%	7%	3%	3%

To what extent do you agree or disagree: The fines imposed as a result of breaching regulations could cripple some organizations

Failure to comply with GDPR brings the threat of fines -- the most severe of which could cost organizations up to 4% of global turnover or €20 million (whichever is greater). Overall, 72% of EU respondents and 78% of U.S. respondents strongly agree or agree that organizations will be hit with considerable fines as a results of GDPR. Respondents in the UK (81%), France (73%) and Germany (63%) were most likely to strongly agree or agree with this statement.

| The fines imposed as a result of breaching regulations could cripple some organizations | 20 | 54 | 16 | 4 | 7 |

■ Agree Strongly   ■ Agree   ■ Disagree   ■ Disagree Strongly   ■ Don't Know
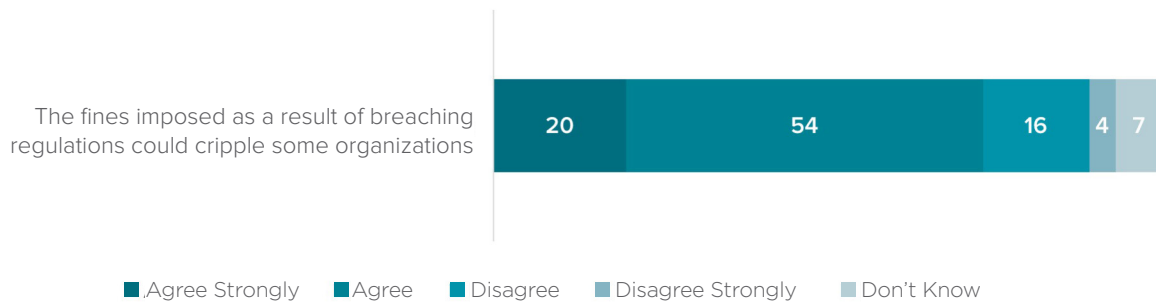
▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Strongly Agree/Agree (Net)	78%	72%	81%	63%	73%
Strongly Agree	25%	18%	19%	14%	20%
Agree	53%	54%	62%	49%	53%
Disagree	16%	16%	9%	23%	14%
Strongly Disagree	1%	5%	1%	9%	5%
Don't Know	5%	7%	9%	5%	8%

To what extent do you agree or disagree: The EU GDPR will not have enough regulators to enforce the mandate

Six out of 10 surveyed in the EU think the GDPR will lack the regulatory enforcement required. The rate of respondents who strongly agreed or agreed was highest in Germany (67%), followed by UK (64%) and France (56%). In the U.S., 47% agreed that the GDPR will not have enough regulators.

| The EU GDPR will not have enough regulators to enforce the mandate | 15 | 42 | 27 | 7 | 10 |

■ Agree Strongly ■ Agree ■ Disagree ■ Disagree Strongly ■ Don't Know
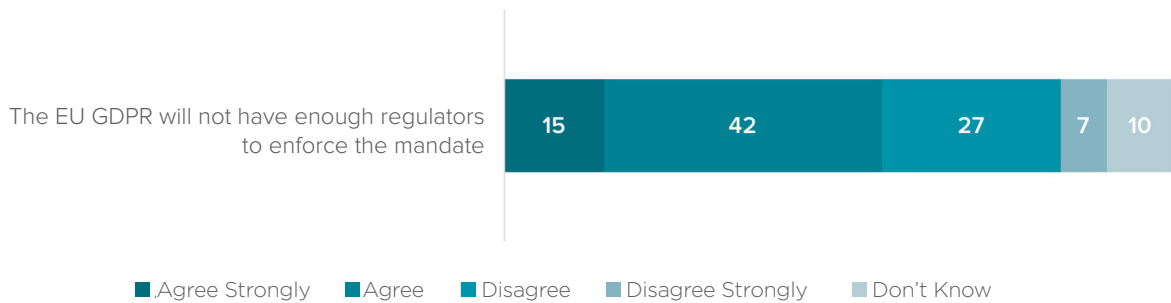
▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Strongly Agree/Agree (Net)	47%	62%	64%	67%	56%
Strongly Agree	16%	14%	14%	16%	13%
Agree	31%	48%	50%	51%	43%
Disagree	33%	24%	23%	22%	25%
Strongly Disagree	9%	5%	3%	5%	8%
Don't Know	11%	9%	10%	6%	11%

To what extent do you agree or disagree: We believe that adhering to the EU GDPR will give us a competitive advantage over other organizations in our sector

About 7 out of 10 organizations in the EU and the U.S. believe that GDPR compliance will give them a competitive edge. Respondents in France (80%) were most likely to strongly agree or agree with this statement, followed by Germany (72%) and the UK (66%). In the U.S., nearly 8 out of 10 agreed.

| We believe that adhering to the EU GDPR will give us a competitive advantage over other organizations | 24 | 50 | 16 | 4 | 6 |

■ Agree Strongly   ■ Agree   ■ Disagree   ■ Disagree Strongly   ■ Don't Know

▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Strongly Agree/Agree (Net)	78%	73%	66%	72%	80%
Strongly Agree	27%	23%	17%	19%	32%
Agree	51%	50%	49%	53%	48%
Disagree	10%	18%	25%	16%	13%
Strongly Disagree	3%	4%	4%	8%	2%
Don't Know	9%	5%	5%	4%	5%

To what extent do you agree or disagree: Our organization does not view compliance with GDPR by the deadline as a priority

Despite the penalties that organizations will face for failing to adhere to GDPR, 4 out of 10 respondents in the EU do not consider GDPR compliance a priority. 41% of the respondents in France, 44% in Germany, and 33% in the UK "strongly agree" or "agree" that their organization does not view compliance with GDPR by the deadline as a priority.

Our organization does not view compliance with GDPR by the deadline as a priority

| 14 | 24 | 35 | 22 | 4 |

■ Agree Strongly   ■ Agree   ■ Disagree   ■ Disagree Strongly   ■ Don't Know

▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Strongly Agree/Agree (Net)	36%	39%	33%	44%	41%
Strongly Agree	11%	15%	13%	18%	15%
Agree	25%	24%	20%	26%	26%
Disagree/Strongly Disagree (Net)	58%	57%	61%	53%	57%
Disagree	34%	36%	37%	36%	33%
Strongly Disagree	24%	21%	23%	16%	24%
Don't Know	6%	4%	6%	3%	2%

* Percentages have been rounded to the nearest whole number

About the Respondents

▼ PRIMARY JOB FUNCTION IN IT

15%
50%
34%

■ Exec Mgmt   ■ Mid Mgmt   ■ Professional
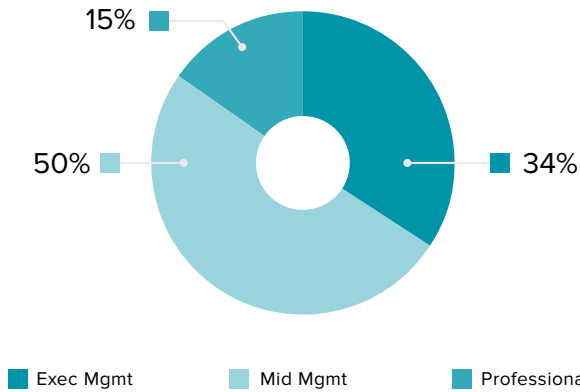
	US	EU	UK	DE	FR
Exec mgmt	24.0%	42.0%	32.0%	38.0%	55.0%
Mid mgmt	58.0%	45.0%	49.0%	55.0%	31.0%
Professional	19.0%	13.0%	19.0%	7.0%	14.0%

Percentages have been rounded to the nearest whole number

▼ ROLE DEDICATED TO CYBERSECURITY

27%
46%
27%
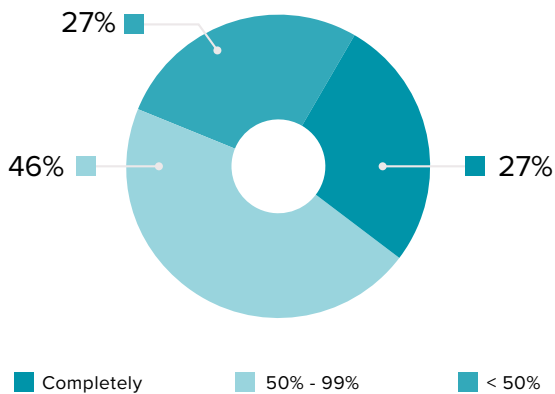
■ Completely   ■ 50% - 99%   ■ < 50%

	US	EU	UK	DE	FR
Completely	28.0%	27.0%	24.0%	27.0%	29.0%
50% - 99%	42.0%	49.0%	44.0%	59.0%	45.0%
< 50%	31.0%	24.0%	32.0%	14.0%	26.0%

▼ FIRM SIZE

	US	EU	UK	DE	FR
1,000 - 1,999 Employees	24.5%	27.7%	24.0%	36.0%	23.0%
2,000 - 2,999 Employees	7.0%	12.7%	12.0%	11.0%	15.0%
3,000 - 4,999 Employees	18.0%	21.3%	50.0%	25.0%	18.0%
5,000 or more Employees	50.5%	38.3%	3.0%	28.0%	44.0%
Don't Know	0.0%	0.0%	2.0%	0.0%	0.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%