Senzing

FINDING
THE
MISSING
LINK
IN GDPR
COMPLIANCE

Foreword

The upcoming EU General Data Protection Regulation ("GDPR") has received a good deal of press attention in recent months. There is a consensus that many businesses will struggle to meet the challenge of GDPR in time for its implementation in May. It was with this in mind that we undertook this major study encompassing businesses large and small across the largest EU economies.

The results reveal an even more alarming picture of GDPR readiness, or lack thereof, than has been reported. Companies have piles of data. Although large enterprises are likely to receive the greatest number of enquiries, the problem is common across companies of all sizes. According to the findings from our research a large proportion of companies – 60% – are not GDPR ready.

Our report finds that it will take days, not hours, to rigorously search all databases and collect all relevant data in order to be GDPR compliant. In the absence of a technological solution, businesses will need to hire in some cases many employees on a full time basis just to handle the volume of data enquiries.

What is most striking to us, however, is that many businesses appear to be sleepwalking towards a GDPR abyss. The fines that can be levied for non-compliance will be potentially terminal to some businesses and even the largest companies – and certainly their shareholders - will feel a significant impact. A huge number of companies simply don't understand the dangers of non-compliance, with a large proportion stating that there would be no, or limited, impact both from a financial penalty and brand reputation perspective.

With almost half of the businesses we spoke to admitting that they were concerned about their ability to be GDPR compliant, there is clearly a lot of work that needs to be done in the next few months. At a bare minimum we believe that 24% of EU businesses should be classed as being seriously "at risk", with a further 36% being "challenged" in terms of meeting GDPR obligations.

At the heart of the problem is the difficulty of locating the data across multiple, often messy, databases. Manually searching will be fraught with error and lead to risk of non-compliance. We think that entity resolution is the only way to discover who is who in companies' data. Without a means to perform a single smart subject search, we envisage many businesses will not be able to comply within the 30-day obligation stipulated by GDPR. In short, companies are holding a compliance time-bomb which only a searchable index can diffuse.

Locating information on individuals, which could be strewn across many disconnected databases, is vitally important. Entity resolution is the missing link in GDPR compliance. This is why Senzing has undertaken this study. Many businesses have not recognised this challenge and the clock is ticking. This report demonstrates the urgency of the situation.

Jeff Jonas,
Founder and CEO, Senzing

Key findings

- 60% of businesses are not "GDPR ready". These are the "GDPR at risk" and "GDPR challenged" groups revealed in the research.

- 44% of businesses from the largest EU economies are concerned about their ability to comply with GDPR.
    - 14% are "very concerned"
    - 60% of large companies are concerned versus 55% of Small and Medium-sized Enterprises (SMEs)
    - Spanish companies are most concerned, with 76% expressing worry

- On average, a company will get 89 GDPR enquiries per month, for which they will need to search an average of 23 different databases, each taking about 5 minutes. The total time spent finding data for GDPR enquiries per month will be more than 10,300 minutes (172 hours). This equates to over 8 hours of searching per working day (or 1 employee dedicated solely to GDPR enquiries).

- The issue is even more pronounced for the largest companies. Those of over 250 employees expect to get an average of 246 GDPR enquiries per month, for which they will need to search an average of 43 different databases, each taking more than 7 minutes. The total time spent finding data for GDPR enquiries per month will be more than 75,500 minutes (1259 hours). This equates to 60 hours of searching per working day (or 7.5 employees dedicated solely to GDPR enquiries every day).

- More than 1 in 10 (12%) of companies are not confident that they know where all their data is housed. This compounds the challenge of scaling what is already a mountain of data collection.
    - Less than half (47%) are "very confident" that they know where all their customer data is housed
    - This is consistent across large and small companies (9% and 11% respectively)
    - French businesses seem particularly concerned that they don't know where all their data is stored, with more than a quarter (27%) saying they're concerned, and only 26% being "very confident"

- 15% of companies are not confident that they have accounted for all the different databases and systems which contain relevant personal/customer data, with only a third (35%) stating they are "very confident".

- There is a noticeable divide between SMEs and large companies. 13% of SMEs are not confident they can account for every database as opposed to only 8% of large companies
    - Again, French companies are most concerned about their ability to account for every database. 30% say they are not confident of doing so and less than a fifth (19%) are "very confident"

- 39% of companies are planning to overhaul IT/customer data systems.
    - Two thirds (64%) of large companies are overhauling their systems compared to only 48% of SMEs
    - Whilst 38% of companies say they plan to do nothing at all as their current set up is already optimum, there is a divide between large and small businesses. 27% of SMEs believe their current set up is optimum, compared to just 16% of large companies, indicating that smaller companies may be underestimating the potential challenge. Micro businesses are the most confident, with 50% saying that their current set up is optimum
    - 15% of companies are hiring data analysts to collect the data. Again, the disparity between large and small companies is striking, with a third (33%) of large companies planning to hire versus less than one in five (19%) SMEs

- Whilst over a third of companies (35%) are aware of the severity of the impact of financial fines imposed by failure to comply with GDPR requirements, worryingly 30% say that financial fines will have no impact at all and 15% say that they "don't know" whether financial fines will have an impact, demonstrating a troubling lack of awareness of the punitive fines facing companies post GDPR implementation.

- More large companies than SMEs understand the severity of the impact of financial fines for GDPR non-compliance. Almost half (47%) think the failure to comply with GDPR will have a severe impact in terms of financial fines levied, as opposed to 38% of SMEs and 29% of micro businesses. Smaller businesses yet again appear to be underestimating the cost of GDPR non-compliance

- Reputational impact is also an area where large companies feel more exposed than smaller companies. Whereas over a third (36%) of all companies polled think that failure to comply with GDPR will severely impact their brand reputation, this concern rises for large companies, with 56% anticipating a severe impact to their brand compared to just 36% of SMEs and 27% of micro businesses

- Given the concerning lack of readiness evident in other responses, companies are paradoxically very positive about their ability to find all customer data within GDPR's 30 day obligation, with 84% claiming that their business will be very or fairly likely to comply.

  - This belief rises to 89% for SMEs and to 92% for large companies. Micro businesses are the least confident (80%)

- Based on an evaluation of the responses:

  - 40% of companies appear "GDPR ready"

  - 36% appear "GDPR challenged"

  - 24% appear "GDPR at risk"

- These readiness ratings are conservative; we believe that the proportion of "at risk" and "challenged" categories may actually be higher in reality.

60%
European companies
not GDPR ready

**THE
GDPR
DATA
ABYSS**

65%
show worrying knowledge gap
around financial penalties

44%
concerned about ability
to comply with GDPR

AT RISK companies facing
tens of billions of €'s of fines

MEDIUM

RISK

LOW

HIGH

24%
businesses in AT RISK category

Sen**z**ing

Background

25th May 2018 is a date etched on the minds of many executives in businesses operating throughout the European Union. Why? This is the day that REGULATION (EU) 2016/679, or to give it its better-known title, the EU General Data Protection Regulation (GDPR), comes into force.

You'd be forgiven for not reading the entirety of the legislation – it runs to some 88 pages and over 55,000 words - but there are some critical changes to previous legislation that will have a seismic impact on businesses operating in the EU.

Created to bring consistency to data privacy laws across the bloc, GDPR replaces the Data Protection Directive 95/46/EC. It aims to protect people from privacy and data breaches which have proliferated in a data-driven world since the original legislation was introduced in 1995.

Some of the important new components of GDPR are:

- Increased Rights for Data Subjects: these enable individuals to request that their data be erased from a company's records, giving them the Right to be Forgotten. They also have the Right to Access, knowing who is collecting their personal information, where this is happening and what is it being used for. Further, the company is obligated to provide a copy of their personal data on request and free of charge, in an electronic format.
  - All requests must be responded to within a 30-day time window.
- The Introduction of Mandatory Breach Notifications: when a data breach which is likely to "result in a risk for the rights and freedoms of individuals" takes place, companies must report this to customers without delay and to data controllers within 72 hours.
- Privacy by Design: data protection must be inherent in the design of all systems, rather than being an add-on.
- Large penalties for non-compliance: penalties will vary depending on the severity of the non-compliance. However, in the most severe cases, companies in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater).

There have been many reports written in the past year alone which have highlighted the unpreparedness of companies ahead of the GDPR implementation date. The majority have focused on the cost of implementation and general levels of preparedness. For example, a January 2018 study by PwC found that 36% of US businesses with large EU operations are still in the assessment phase regarding the costs and requirements for GDPR compliance, risking huge fines, litigation costs and lost contract opportunities for EU businesses[1].

Furthermore, a survey of 284 retail websites carried out in November last year by international law firm Bryan Cave found that every company polled would have failed GDPR requirements in some way[2].

This report shows that, worryingly, the situation has not progressed and, in fact, could be worse than feared.

It is evident that the scale of the challenge for companies remains vast and, ominously, our new research suggests that there remains no great sense of urgency ahead of the GDPR implementation date. Indeed, there is a concerning complacency, particularly prevalent in certain countries, when it comes to data subject requests and the necessary data collection requirements to meet these requests within the 30-day deadline.

The focus of this report is primarily on Data Subject Rights and the obligations companies will be under from 25th May in this area. The biggest hurdle as we approach the deadline is that company databases are often discrete, disorganised and prone to duplications and input errors. In short, many databases are not smart. Compliance will be a challenge – perhaps impossible – even if there is a dedicated compliance or risk team if there is no means to perform a single subject search.

Basically the major issue is locating individual data subjects through the labyrinth of data. In order to fix this situation and address the Missing Link, companies need understand Entity Resolution.

GDPR compliance starts with one simple question: "What do we know about the data subject?" Unfortunately, this is an exceptionally hard question for organisations to answer. This is because a lot of companies have many databases, some of which they may even be unaware of, and manual search is unreliable. For example, although a customer has requested their data, it may be that they have a record in another non-customer file; perhaps they applied for a job at your company last year, so you would need to check the HR database. Perhaps they are a member of a loyalty club. Also, are you confident that you have all of their details? Have you checked the multiple derivations of their name, including married names/maiden names and potentially misspellings, factoring in typos and human error? The challenge of data collection is therefore enormous.

The key for companies is smart Entity Resolution in their data collection. In simple terms, resolving who is who in your data, quickly and cost effectively. We think this has largely been overlooked. As the GDPR deadline looms there is an alarming sense of confusion and lack of confidence about data collection which could result in large fines and reputational damage which, in some cases, could be existential.

> **"The biggest hurdle as we approach the deadline is that company databases are often discrete, disorganised and prone to duplications and input errors. In short, many databases are not smart."**

1 https://www.pwc.com/us/en/increasing-it-effectiveness/publications/general-data-protection-regulation-gdpr-budgets.html
2 https://www.bryancave.com/en/news-events/bryan-cave-research-reveals-100-of-retail-websites-surveyed-are.html

Overall concern about GDPR compliance

Almost half (44%) of organisations from the five largest EU economies declare themselves to be "concerned" about their ability to comply with GDPR. This gives an indication of the scale of the challenge facing many companies between now and May this year. Indeed, 14% say they are "very concerned".

When analysing the responses from different sizes of companies a pattern emerges that becomes increasingly evident throughout this report – namely that smaller companies tend, at best, to underestimate issues relating to data protection and GDPR and, at worst, have their heads in the sand.

- 60% of large companies say they are concerned about their ability to comply with GDPR

- This compares with 55% of SMEs and 34% of micro businesses

There is also a marked divide in the attitudes demonstrated in different EU countries. It appears that there is a particular problem in Spain, where 76% of executives say they are concerned about their organisation's ability to be GDPR compliant. Alarmingly, 41% say that they are "very concerned" about GDPR compliance.

The next most concerned countries are Italy, with 43% of Director-level business people voicing anxiety, and the UK (39%). France and Germany seem slightly less worried, with 31% and 33% respectively indicating concern.

Jeff Jonas, Founder and CEO, Senzing said "With less than four months to go until GDPR becomes law the fact that almost half of companies operating in the EU are concerned about their ability to comply is a huge red flag. It will not only be company management teams which are fretting, but shareholders will also be unnerved by these figures. Considering larger companies are the most concerned, many sizeable listed enterprises could face huge fines and their valuation would suffer. Large Spanish entities look particularly vulnerable."

CONCERNS OVER ABILITY TO BE GDPR COMPLIANT

Large companies

SMEs

All companies

Micro businesses

60% **55%** **44%** **34%**

The scale of the data collection challenge

In order to get a real sense of the scale of the data gathering challenge we wanted to drill down to the operational level, asking executives to state how many databases they have which would house GDPR-relevant data, the amount of time it would take them to conduct a search of a single database and how many GDPR enquiries they anticipate receiving per month. Armed with this data, we can calculate the total quantum of time per month that a company will have to spend solely searching its databases.

The results are telling. The sheer volume of data to be searched is staggering. As expected, there is a significant difference between large companies, which expect a huge volume of enquiries and have many complicated databases to search, and SMEs and micro businesses, which have a smaller task but still require a substantial time expenditure.

THE GREAT DATA COLLECTION CHALLENGE

	Average enquiries per month	Average number of databases	Average minutes per enquiry	Total minutes per month	Total hours per working day
All	89	23	5 minutes, 2 seconds	10,317	8 hours, 11 minutes
Large	246	43	7 minutes, 8 seconds	75527	59 hours, 56 minutes
SME	15	18	4 minutes, 58 seconds	1339	1 hour, 3 minutes
Micro	7	9	3 minutes, 2 seconds	191	9 minutes
All companies above 10 employees	131	31	6 minutes, 3 seconds	24569	19 hours, 30 minutes

On average, a company will get 89 GDPR enquiries per month, for which they will need to search an average of 23 different databases, each taking about 5 minutes. The total time spent finding data for GDPR enquiries per month will be more than 10,300 minutes (172 hours). This equates to over 8 hours of searching per working day (or 1 employee dedicated solely to GDPR enquiries).

The issue is even more pronounced for the largest companies. Those of over 250 employees expect to get an average 246 GDPR enquiries per month, for which they will need to search an average of 43 different databases, each taking more than 7 minutes. The total time spent finding data for GDPR enquiries per month will be more

than 75,500 minutes (1259 hours). This equates to nearly 60 hours of searching per working day (or 7.5 employees dedicated solely to GDPR enquiries every day).

Whilst micro businesses expect a small number of enquiries and have a comparatively small number of modest databases to search, when these companies are excluded from the sample the challenge faced by businesses with more than 10 employees is brought into stark relief - almost 20 hours a day of extra work equating to two and a half full time employees. Even SMEs will need an employee to dedicate an eighth of the working day simply to trawl through disparate databases to retrieve relevant customer data.

Jonas continues: "These findings reveal the true extent of the GDPR compliance challenge. Businesses will be faced with a mountain of data to trawl through - the end result will be a significant time and personnel cost and a great risk of missing records or worse, including the wrong records. Whilst this time requirement is most onerous for large companies, they have greater resources at their disposal. Relative to size, SMEs face a similarly gargantuan task. For a company of 10 people, to have a single person dedicating 22 hours or so per month solely on database searching represents measurable expense."

AVERAGE NUMBER OF GDPR ENQUIRIES A COMPANY EXPECTS PER MONTH
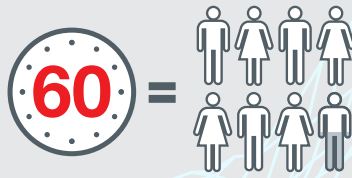
89
Average company

246
Large companies

HOURS PER WORKING DAY DEDICATED TO GDPR DATA COLLECTION

8 =
Average company
8 hours = 1 full time employee

60 =
Large companies
60 hours = 7.5 full time employees

? **?** **?**

15%
are not confident they have accounted for all the different databases

?

12%
are not confident they know where all their data is housed

Entity Resolution required

The scale of the GDPR data challenge

Sen**z**ing

Compounding the problem

Although the size of the task simply to search all of the requisite databases for all enquiries is Herculean in itself, it is made even more difficult by the fact that a significant proportion of businesses appear to be unsure of where relevant data might be kept and are unaware of all the pertinent databases.

More than 1 in 10 (12%) companies say they are not confident that they know where all their data is stored. This compounds the challenge of scaling what is already a mountain of data collection. Indeed, less than half (47%) are "very confident" that they know where all t heir customer data is housed.

Similarly, 15% of businesses are not confident that they have accounted for all the different databases and systems which contain relevant personal/customer data, with only a third (35%) stating they are "very confident".
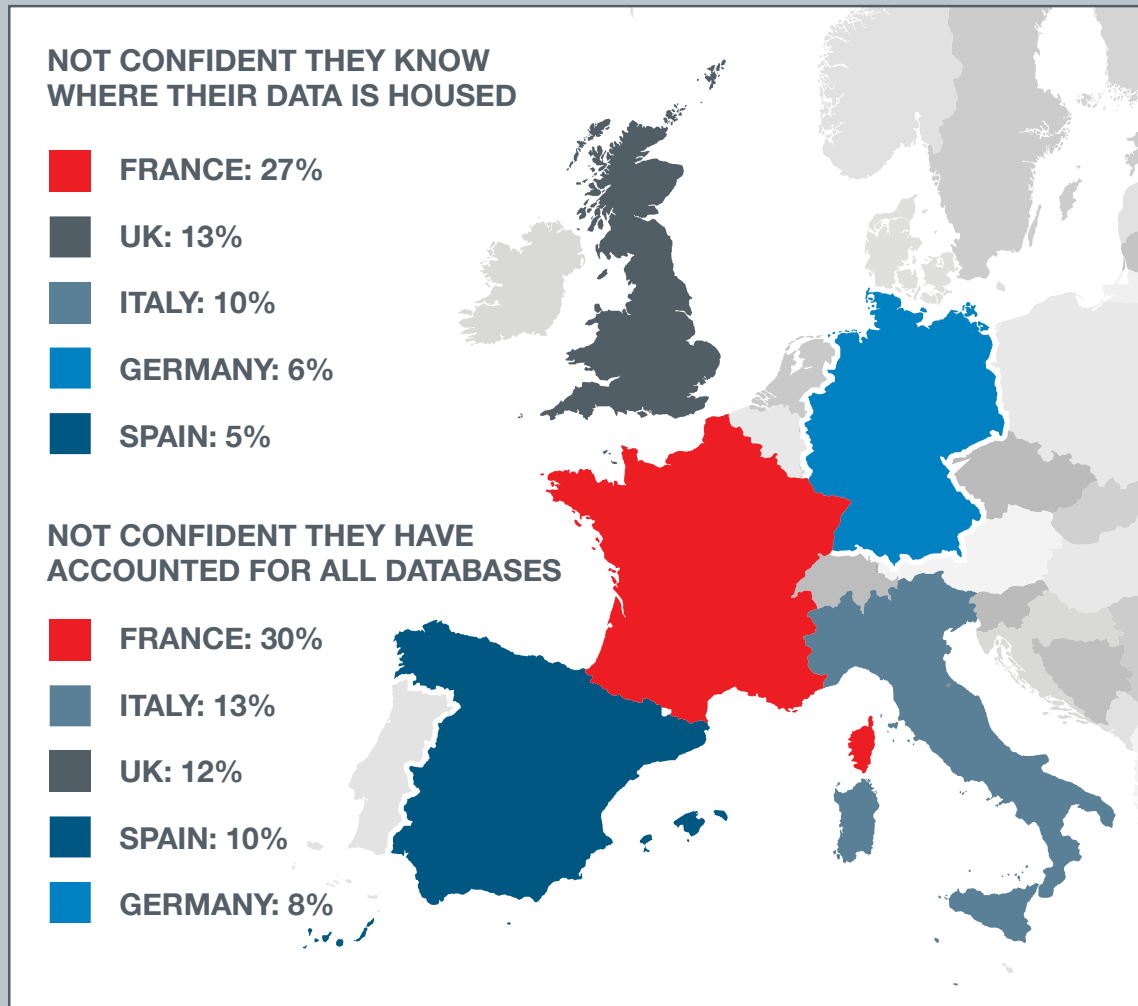
Whilst the level of confidence in knowing where data is housed is fairly consistent across large and small companies (9% and 11% respectively), there is a more noticeable divide between large enterprises and SMEs when it comes to concern that they have not accounted for all pertinent databases; whereas only 8% of large companies are not confident in this regard, 13% of SMEs expressed worries, rising to 18% for micro businesses.

Moreover, certain countries and sectors seem particularly exposed in terms of being aware of where data is housed and of all databases that they use. French businesses seem especially concerned that they don't know where all their data is stored, with more than a quarter (27%) saying they're concerned, and only 26% stating they are "very confident". 30% say they are not confident in their ability to account for every database and less than a fifth (19%) are "very confident".

The retail sector is expected to be at the sharp end of GDPR compliance, given the volume of customer data and marketing activity – particularly for those with a large online operation. It is alarming therefore that 16% of retail companies are not confident that they know where all their data is housed and one in five (19%) are not confident that they have accounted for all of their databases.

Jonas adds: "You can't search what you can't find. Finding out who is who and where their data is should be the first principle of GDPR compliance. This is why we think Entity Resolution is mission critical for companies. Our worry is that, in investing in systems, processes and personnel, many companies are attempting to reach bases two, three and four without first getting to first base. At this stage in the GDPR timeline you would expect most companies to be very confident about knowing the location of all of their data but the reality is that businesses which feel this are in the minority."

Accounting for all databases

NOT CONFIDENT THEY KNOW WHERE THEIR DATA IS HOUSED

- **FRANCE: 27%**
- **UK: 13%**
- **ITALY: 10%**
- **GERMANY: 6%**
- **SPAIN: 5%**

NOT CONFIDENT THEY HAVE ACCOUNTED FOR ALL DATABASES

- **FRANCE: 30%**
- **ITALY: 13%**
- **UK: 12%**
- **SPAIN: 10%**
- **GERMANY: 8%**

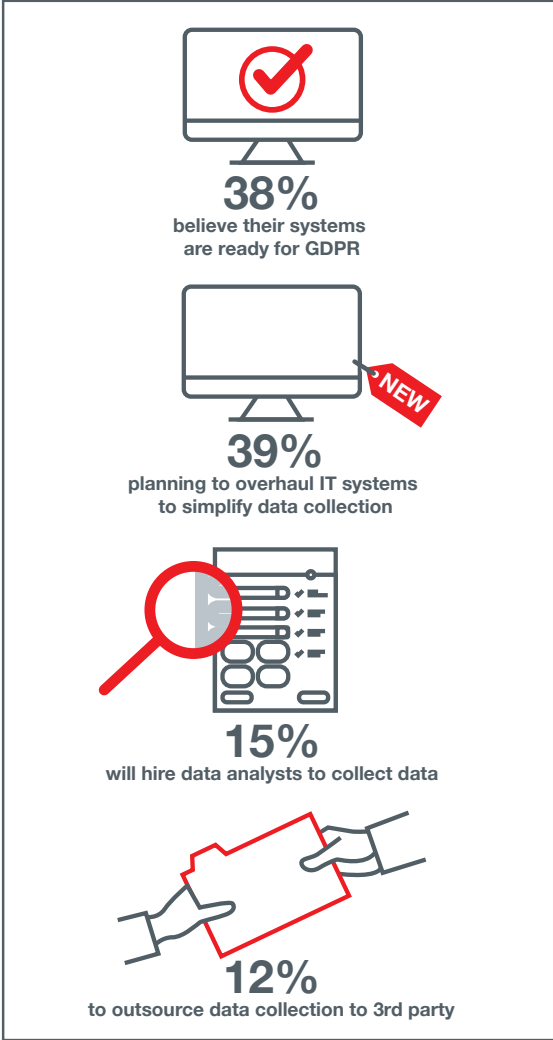# How companies are planning to address the challenge

Although there is encouraging evidence of companies taking affirmative action to become GDPR compliant, there is also a troublingly high number of companies which either do not know what actions they are taking or believe that they are already set up to meet the challenge.

38% of companies say they plan to do nothing at all as they believe their current set up is already optimum and, whilst this will undoubtedly be true in some cases, in others it may be a case of false optimism. There also seems to be a significant divide between the attitudes of large and small businesses. A quarter (27%) of SMEs say their current set up is optimum, compared to just 16% of large companies who believe this, indicating that smaller companies are underestimating the potential challenge. Micro businesses are the most confident, with 50% saying that their current set up is optimum.

In terms of what actions organisations are planning to take ahead of May, the most prevalent is an overhaul of IT/customer data systems, with 39% of companies planning to take this step. The divide between large and smaller businesses is again evident. Two thirds (64%) of large companies are overhauling their systems compared to only 48% of SMEs.

15% of companies are hiring data analysts to collect the data. Once more the disparity between big enterprises and SMEs is striking, with a third (33%) of the former planning to hire versus less than one in five (19%) of the latter.

Tech companies seem most attuned to the need to make significant operational changes in order to be GDPR compliant, with only a quarter (27%) saying that their current set up is sufficient, compared to the 38% average across all businesses. Mirroring this trend, 58% of tech companies are planning to overhaul their IT/customer data systems compared to an average of 39% across all companies. Furthermore, 29% are planning to hire more data analysts, compared to 15% average across all sectors.

38%
believe their systems are ready for GDPR

NEW

39%
planning to overhaul IT systems to simplify data collection

15%
will hire data analysts to collect data

12%
to outsource data collection to 3rd party

	Overhaul IT/ customer data systems	Hire data analysts to collect the data	Outsource data collection to a third party	Nothing at all – our current set up is optimum	Don't know
All companies	39%	15%	12%	38%	12%
Large companies	64%	33%	22%	16%	3%
SMEs	48%	19%	15%	27%	5%
Micro	27%	6%	7%	50%	17%

*This was multiple choice and respondents were invited to select all actions that applied to their business

Jeff Jonas says: "The fact there is such a distinction in the level of confidence between large and small companies in their existing data collection set up is disturbing. It suggests strongly to us that SMEs and micro businesses are seriously underestimating the impact that GDPR will have on their systems and are demonstrating misplaced optimism. Getting it wrong could potentially be terminal some businesses. Most smaller companies are not yet ready."

The awareness gap – sleepwalking towards a financial and reputational abyss

In the responses related to the actions a company needs to take in preparation for GDPR, a pattern began to emerge: many businesses – particularly smaller ones – appeared to believe that their status quo is optimum. We see a similar picture in companies' responses about the financial and reputational impact of GDPR non-compliance, with a worryingly high proportion unaware of the ramifications or, more concerningly, claiming there is little or no impact. This is a startling claim in light of the heavy fines which will be levied in the event of non-compliance. It is perhaps evidence that many companies' optimism and confidence in their preparedness is not grounded in reality.

Whilst over a third of companies (35%) are aware of the severity of the impact of financial fines imposed by failure to comply with GDPR requirements, an alarming 30% say that financial fines will have no impact at all and 15% say that they "don't know" whether financial fines will have an impact. These findings serve to demonstrate a lack of awareness of the punitive fines facing companies post GDPR implementation - €20 million or 4% of global annual turnover (whichever is greater) in the worst cases.

Mirroring a similar pattern to other findings in this report, smaller businesses appear to have less appreciation for the seriousness of GDPR and the importance of adhering to the new rules. A greater proportion of large companies compared to SMEs understand the severity of the impact of financial fines for GDPR non-compliance. Almost half (47%) believe that the failure to comply with GDPR will have a severe impact in terms of financial fines levied, as opposed to 38% of SMEs and 29% of micro businesses. Smaller businesses yet again appear to be underestimating the cost of GDPR non-compliance.

The impact on a company's reputation – that intangible but vital asset – is also an area where large enterprises feel more exposed compared to smaller companies. Whereas over a third (36%) of all businesses polled think that failure to comply with GDPR will severely impact their brand reputation, this concern rises for large companies, with 56% anticipating a severe impact to their brand compared to just 36% of SMEs and 27% of micro businesses.

Given the concerning lack of readiness evident in other responses, companies are paradoxically very positive about their ability to find all customer data within GDPR's 30-day obligation. The overwhelming majority of organisations polled (84%) claim that their business will be very or fairly likely to comply with the new legislation. This belief rises to 89% for SMEs and to 92% for large companies. Micro businesses are the least confident (80%).

Jonas comments: "Given that many respondents cited a lack of awareness about where their data is housed, expressed concern that they did not know where all their databases are located, appear ignorant of the possible fines that could be incurred and maintain a belief that no improvements to existing systems are needed in advance of the deadline, the positivity around meeting the 30-day obligation seems unjustifiably high. There is a danger that companies are acting in hope rather than expectation. They risk sleepwalking towards a GDPR abyss."

	Severe impact	Awareness gap
Large companies	47%	53%
SMEs	38%	62%
All companies	35%	65%
Micro businesses	29%	71%
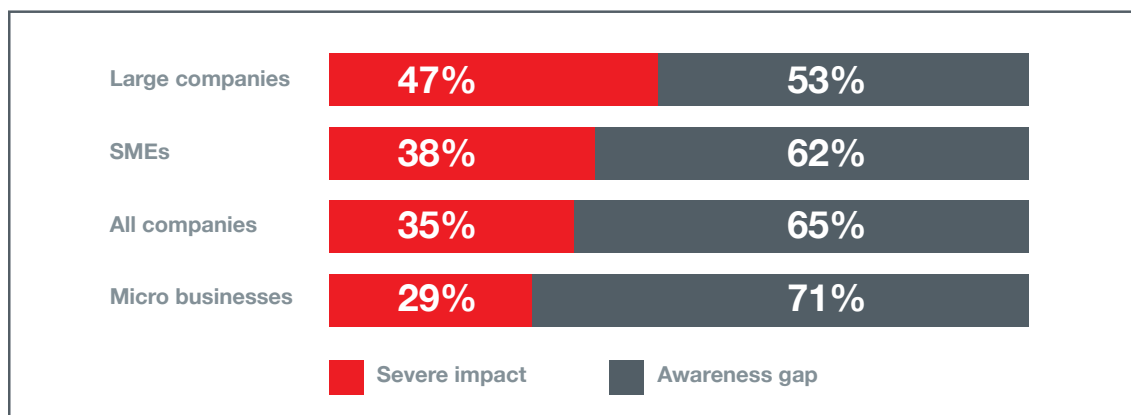
Conclusion

The findings of this report identify a number of key themes for businesses operating in the EU as the GDPR implementation date grows nearer:
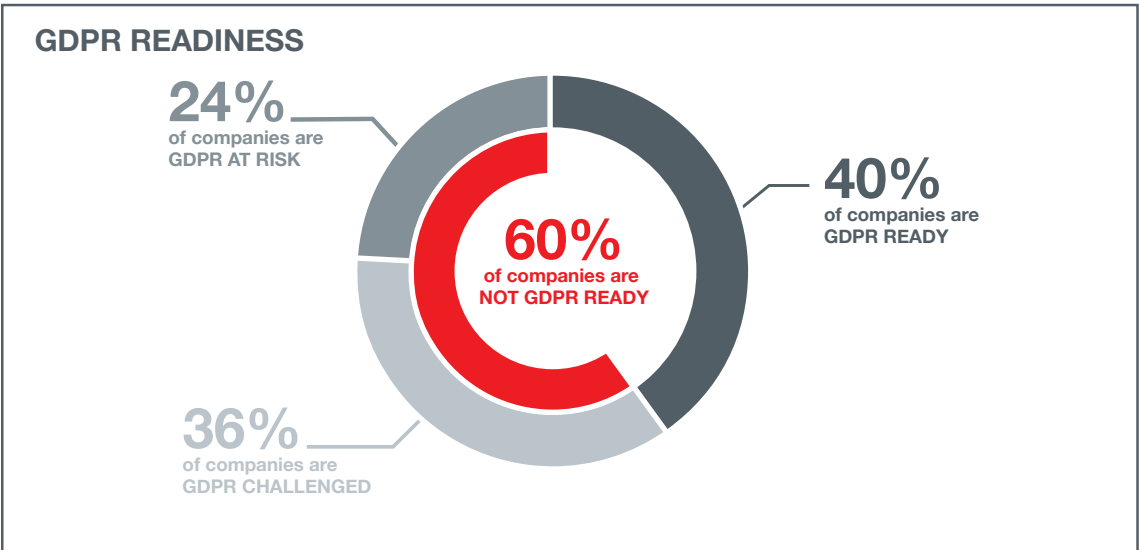
- **Lack of readiness is rampant.** 60% of all companies are not GDPR Ready for dealing with the challenges that GDPR compliance will demand.

- **Underestimated time to find data.** The sheer amount of time it will take companies to search all of their relevant databases and handle all enquiries within the 30-day obligation is mammoth; it will come as a shock to many of them. It will require, in many cases, dedicated staff and strategic decisions around operations.

- **The knowledge gap.** There is a concerning knowledge gap in relation to data whereabouts, and a lack of understanding of the implications of non-compliance. Knowledge is inversely correlated with confidence, indicating that many companies' optimism is potentially unjustified.

- **SMEs are especially at risk.** Large companies are more awake to the scale of the challenge than their smaller counterparts. SMEs need to ensure that they are truly taking adequate steps to prepare for the new data paradigm.

- **Confidence is mixed.** Some EU countries seem particularly exposed to GDPR risk. Spanish companies are extremely worried about their ability to comply with GDPR, whilst French companies are the least confident about where their data is located.

- **Effective entity resolution is needed.** A huge amount of money and time will be expended on overhauling IT systems. This should help to solve a part of the GDPR puzzle but it will not provide a silver bullet solution; it is very unlikely that this will address the "messiness" of databases themselves and, with that, enable effective entity resolution.

Based on an evaluation of the responses to questions throughout the research, we have devised a broad rating of companies' GDPR readiness.

Despite the eye-catching figures, our view is that the proportion in the "at risk" and "challenged" categories is actually lower than the reality. We believe the number of businesses in these categories is likely to be higher because our calculations factor in some responses which are based on an optimism which is possibly overstated.

Our findings point towards the fact that the missing link in GDPR compliance is Entity Resolution. Companies are overlooking the urgent need to be able to perform a single smart subject search to find out who is who in their data. Without Entity Resolution, the critical enabler of GDPR readiness, many businesses will be unable to meet the demands of GDPR.

GDPR READINESS

24% of companies are GDPR AT RISK

40% of companies are GDPR READY

60% of companies are NOT GDPR READY

36% of companies are GDPR CHALLENGED

Responding to the findings, Dr James Canton, CEO and Chairman of the Institute for Global Futures, said: "In GDPR we are entering a new data paradigm and this research shows that thousands of companies across the EU do not understand the extent of the change and are not ready for this brave new world. The fact that a quarter of businesses are categorised as being 'at risk' is truly shocking and logically means potentially tens of billions, if not hundreds of billions, of euros in fines could be levied. The future of smart data collection lies in entity resolution used with big data analytics and machine learning AI. Without machine learning entity resolution businesses will not be able to cope with the tsunami of data.

"This is more than simply about being GDPR compliant. Society is unprepared for knowledge extraction and the demands for faster decision-making that our customers and markets, our planet, will require for high performance, competitive advantage and likely survival in the future. For those businesses which successfully learn to harness the power of Big Data Intelligence great rewards await. For those that don't, large fines, declining market share and, ultimately, oblivion beckons."

Methodology

The report is based on a survey of 1,015 companies. These companies are based in UK, Germany, France, Spain and Italy and all respondents were polled in their native language. There was a representative spread across sectors, countries and size of businesses.

When the report refers to "large businesses" it means those companies employing more than 250 people. The term "SME" is used to refer to businesses employing between 10 and 249 companies. "Micro businesses" are all companies employing between 0 (i.e. self-employed) and 9 people.

Respondents from large businesses were selected on the basis that they were responsible for, partly responsible for, or had influence over, data protection regulations within their firm, or a good working knowledge of their firm's data protection compliance. Respondents from SMEs and micro businesses were selected on the basis of seniority (management or board level).

The research was conducted by Populus, the research house, between 9 and 15 January 2018.

The GDPR readiness scale is calculated on the basis of responses to questions which are explicitly about knowledge, understanding and actions being taken in relation to GDPR.

These are:

- Level of knowledge of where data is housed

- Level of confidence about being able to account for all different databases

- Actions being taken to prepare for GDPR

- Level of awareness of reputational impact of GDPR non-compliance

- Level of awareness of financial fines resulting from GDPR non-compliance

- Level of confidence that the company can be respond to data enquiries within the 30-day obligation

The responses were apportioned the label of "ready", "challenged" or "at risk", dependent on the level of knowledge, understanding or activity demonstrated.

Example 1: When asked "How confident or not confident are you that you know where all your customer data is housed", a response of "not at all confident/not very confident" was classed as "at risk"; a response of "fairly confident" was classed as "challenged"; a response of "very confident" was classed as "ready".

Example 2: When asked "How much of an impact do you think failure to comply with GDPR will cost your business in terms of financial fines?", a response of "don't know" or "no impact at all or very limited impact" was classed as "at risk"; a response of "fairly severe" was classed as "challenged"; a response of "severe impact" was classed as "ready". We have classed this in such a way because the size of financial fines relating to GDPR is well-publicised and should be well known to all businesses, so those that do not think there is a serious impact are viewed as lacking critical knowledge and therefore exposed.

Using this classification system, the number of responses in each category was aggregated and a mean average taken. This mean average was then applied as a percentage of the overall 1,015 respondents to the survey to give the proportion of companies that are "GDPR ready", "GDPR challenged" and "GDPR at risk".