GDPR: BEST PRACTICE FOR DATA PROTECTION IN THE INFORMATION AGE

Skillsoft | sumtotal A Skillsoft Company

HR review

General Data Protection Regulation (GDPR) is a watershed moment for data security and citizens' rights. After four years of discussions, the new regulation was ratified in December 2016 and will go live in all European Union (EU) member states on the 25th May 2018. But what does it mean exactly? What are its principles? And what are the best ways for organisations to ensure they are compliant? This whitepaper will clarify the details around GDPR and offer best practices for companies to implement.

GDPR is applicable to any organisation of a certain size that handles or processes personal data in the act of trading goods and services within the EU. In other words, if you are a business with more than 250 employees, and you handle or store personal data, you will be obliged to comply. The ultimate aim of GDPR is to bring data protection protocols up to speed with the new and unprecedented ways in which information is now used. It also looks to empower individuals (or 'data subjects') by giving them the right to challenge how, what, when, and why data is held about them. Data subjects have the right to access any information a company holds on them, and the right to know why and how that data is being processed, how long it's stored for, and who gets to see it.

GDPR'S GLOBAL INFLUENCE

You could be forgiven for thinking that international companies outside of the EU are free of any obligation to comply, but this would be mistaken. Even if an entity is not physically located within the jurisdiction, they are still expected to comply if they handle personal data that is identifiable to a resident that is located within the EU. This extraterritorial effect means that GDPR will likely have a truly global influence, forcing international companies with less judicious data protection to improve their practices, so as not to jeopardise established trading ties within the jurisdiction and incur penalties for failure to comply.

WHY CURRENT DATA PROTECTION ISN'T SUFFICIENT?

Current legislation was enacted long before the sophisticated technologies of today were invented. In 1995, for example, data was at far less risk of exploitation because things like cloud technology and mobile connected devices simply didn't exist—or at least not in the same capacity as they do now. The EU wants to develop a greater sense of trust in the emerging digital economy by bolstering protection, for both individuals and businesses, based on the latest technological capabilities available. But it also wants to give organisations a more straightforward legal framework in which to operate by making the protocols identical throughout the region.

Currently, the UK uses the Data Protection Act (DPA) of 1998 as its framework for data security. The DPA was ushered in after the EU's own 1995 Data Protection Directive. GDPR will ultimately replace both of these and act as one harmonised data protection undertaking across the entire jurisdiction of the EU. The fines and penalties that result from failure to comply are much harsher than previous regulation, demonstrating how serious GDPR will be taken by auditors, inspectors, and businesses alike.

GDPR will ultimately give legal structure and greater protection to citizens in the wake of the rapid advances in technology and data usage since the last century. The "information age" is aptly named—nowadays data is collected on an unprecedented scale that could not have been foreseen even just 20 years ago. It is also valued, traded, and manipulated in similar ways to global currency – making it ideal and highly prized to those with nefarious intentions. This data explosion has undoubtedly helped commerce prosper in the 21st century, but it has also given rise to countless risks and opportunities for serious breaches. In this era, data is just as likely to be abused, as it is to be legitimately used. Indeed, as research from the Breach Level Index demonstrates, over nine billion records have been lost or stolen since 2013, of which "only 4% were 'secure breaches' where encryption was used and the stolen data was rendered useless". This figure equates to 59 records being stolen every single second. It's because of this worrying statistic that GDPR has been drafted.

IMPACT OF THE UK'S DEPARTURE FROM THE EUROPEAN UNION

Whilst GDPR is centered on simplifiying business and data protection across the entire European Union jurisdiction, its core principles will still apply to the UK regardless of the exact outcome of the 'Brexit' negotiations. The UK Government has repeatedly made clear that GDPR will essentially be transposed into UK law (some amends notwithstanding) by the time an official exit is made on the 31st March, 2019. In other words, the UK will essentially 'mirror' GDPR post 'Brexit' to ensure that data continues to flow unrestricted between the UK and EU member states – a critical factor to the ongoing prosperity of the digital economy.

GDPR will also, however, become active long before the UK formally cuts ties with EU. This 10-month crossover period between GDPR's 'live' date (25th May, 2018) and the UK's change of status as an EU member state (31st March, 2019) means that businesses based in the UK will still need to comply and do everything they can to get their 'houses' in check. Those that fail to do so can expect fines of up to £17 million, or 4 per cent of global turnover, whichever is highest.

THE 7 CORE PRINCIPLES OF GDPR

Before looking at recommendations for best practice, it's instructive to first be clear about the principles that underpin GDPR. Doing so will give business leaders a solid understanding of why these changes are taking place and how best to execute plans to ensure their organisations remain compliant and lawful. A better understanding of these principles also helps companies to become more familiar with the language around GDPR and how best to communicate strategy with employees.

Like previous data protection regulation, GDPR still distinguishes between controllers and processors—controllers dictate how and why personal data is processed, whereas processors act on the controller's behalf. In reality, a controller could be any organisation—a private company, charity, or other body. As for the processor, this could be an IT company or individual hired-hand that is responsible for archiving, maintaining, and actioning an organisation's data.

Some might see this relationship as imbalanced in terms of accountability, but GDPR still places a burden of responsibility on both roles with the legal implications for poor practice clearly outlined on each side.

GDPR has seven fundamental principles to ensure the individual's rights and security of sensitive personal information that could be used for illegitimate purposes. GDPR regularly makes reference to the the term 'data subject' – this is used to describe a living individual to whom personal data relates. In other words, the data subject is a uniquely identifiable human being.

1 ACCOUNTABILITY

The data controller(s) must show that an organisation's data processing remains in line with the six following GDPR principles at all times. Furthermore, it must be clearly demonstrable to Data Protection Agencyinspectors that an organisation is doing everything it reasonably can to comply.

2 ACCURACY

Accuracy demands that the data a company holds on file about an individual should be entirely accurate and kept fully up to date. Any inaccuracies or outdated information should be amended (or deleted, if appropriate) in a timely fashion. GDPR asks "every reasonable step" be taken to achieve complete data accuracy.

3 DATA MINIMISATION

Minimisation means that data collected should be adequate and limited to what is absolutely necessary in order to perform the task the information is intended for. Using information to perform extra tasks outside of original intended purpose (without asking the data subject first) would contravene GDPR's notion of consent.

4 INTEGRITY AND CONFIDENTIALITY

This is the 'individual principle'. Data processing must assure the security and privacy of the data subject at all times. In other words, a company's network security should be sufficient enough to assure the privacy of the data subject's information. In the event of a breach, the company must inform all affected individuals using an appropriate breach notification procedure. Notification must be carried out within 72 hours of becoming aware of a breach.

5 LAWFULNESS, FAIRNESS, AND TRANSPARENCY

All personal information should be processed lawfully. Lawfully can mean (but is not limited to): in accordance with a contract or legal obligation; the processing of data is within the public interest; data processing is in the controller's legitimate interests, such as preventing illegal activity or a breach. Moreover, personal data should be processed fairly and transparently. It should also be easily communicated to the data subject if they request. Controllers have a window of roughly one month to respond to a subject access request.

6 PURPOSE LIMITATION

Personal information collected by an organisation must have a lawful and legitimate purpose behind it. Superfluous information that has no specific function – for example 'extra' data that is used to formulate a more detailed picture of individual consumer habits or preferences – would constitute as illegitimate. Additional processing tasks that are incompatible with the original intended purpose would constitute as unlawful without further permission of consent from the data subject (as per the minimisation principle).

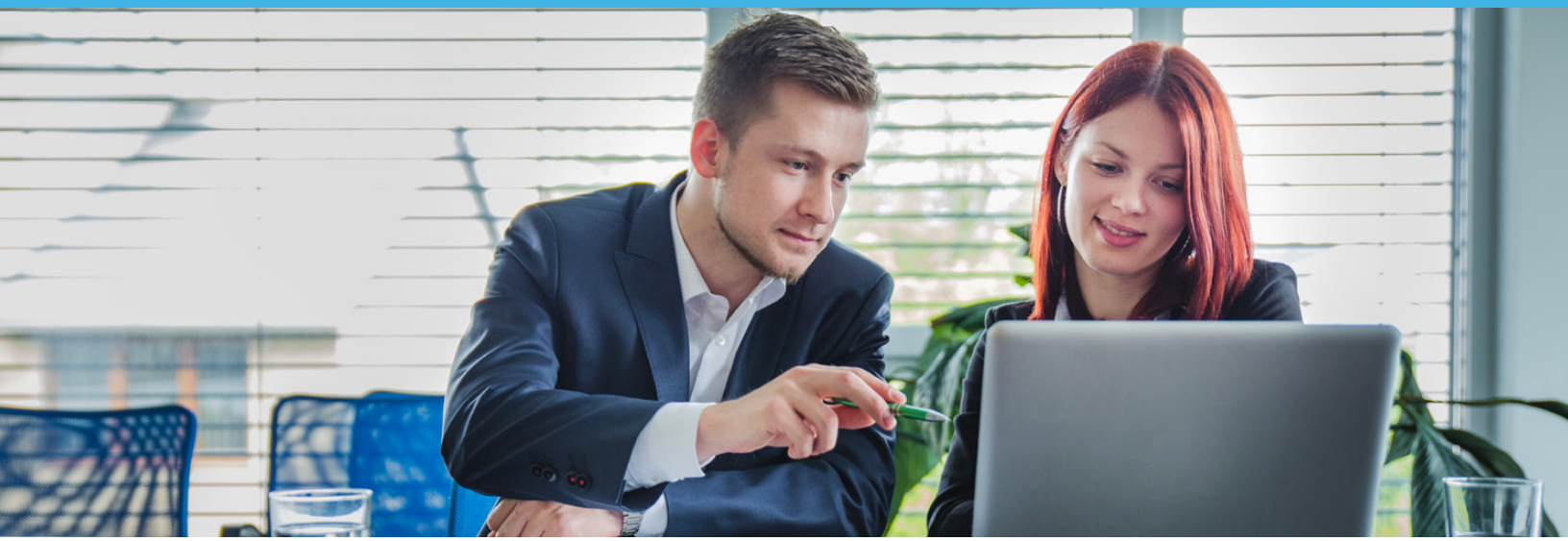
7 STORAGE LIMITATION

Storage limitation asks organisations not to hold personal information for longer than is absolutely necessary or outside the purposes for which it was first collected. Data destruction should be safe and secure.

Corporate data protection strategy that is drafted with these seven principlesin mind will go a long way towards achieving a compliant position when GDPR takes effect.

WHAT IS A SUBJECT ACCESS REQUEST?

Individuals (i.e. data subjects or employees) have the right to be informed by an organisation, most often their employer, if it is processing any personal data that relates to them. If it is, they must notify the individual: what data is being processed; a legitimate purpose for why it is being stored and processed; who this data is disclosed to, if any; and the reasons beind any automated processing. Subject access requests must be returned by the organisation in an intelligible form and include copies of the information and how this information was sourced. Organisations have a 40 day window to respond.



HOW DOES GDPR AFFECT HR?

With GDPR affecting the privacy and rights of the individual, the implications for HR are likely to be pronounced. One of the biggest challenges for HR professionals, especially those that deal with applicant data, will be assuring an organisation gains clear consent from the data subject. Consent must be an active and affirmative action by the individual, not a passive or tacit acceptance. As such, pre-ticked boxes or opt-outs will not be viewed favourably by inspectors. Consent can be removed by the data subject as they see fit, further complicating matters for HR departments. Controllers must keep a log of when consent was given and when it was rescinded. A quick win for HR departments looking to become fully compliant will be eliminating 'pre-agreed' options from company literature and instead putting measures in place that obtain unequivocal consent from the data subject. HR professionals should also immediately stop collecting information via old or non-compliant methods. Doing so now will save hours of confusion and wasted time.

The impact for HR goes beyond consent. HR departments work with all types of data, not just from current employees but former and prospective ones too. The source from which this information is collected will vary from department to department, let alone business to business. Often information will come electronically, via online forms or emailed documents, but paper filing is still commonplace.

It's important to keep hard copies and deal with any non-compliant paperwork immediately This typically means disposal. Another quick win for HR personnel looking to strengthen their GDPR compliance will be migrating company practices away from paper-based to digital.

Hard-copy filing is laden with risk, let alone outdated, and it's time for HR departments to initiate this change if they haven't done so already. In instances where it is statutorily necessary to keep hard copies on file, HR should make it a priority to ensure there is nothing contained within that could cause a problem with inspectors.

Further still, HR professionals must now also consider how transparency, access rights, and retrieval of data can be successfully worked into their remit. Under GDPR, individuals can request what information is held about them and why, as such departments will need to consider how current practices assist with this and what changes need to be made in order to be compliant.

The following is a list of major concerns that HR departments will need to resolve as they prepare for GDPR. Though not exhaustive, addressing these questions will go a long way towards achieving full compliance.

RECRUITMENT

Do applicants receive an appropriate privacy notice, detailing how, why, and what their data will be used for? Is the data collected absolutely necessary? Do these forms provide an opportunity for the applicant to give express consent? Are background checks proportionate and only carried out once a job offer has been made? Does the company work with any other party during the recruitment process? Are they compliant?

SUBJECT ACCESS

Is company procedure robust enough to manage incoming access requests? Can the company disclose these transparently.

PRIVACY STATEMENTS

Do employees receive adequate notice of how the company intends to use a subject's data? Does this statement explain their rights clearly and coherently?

IMPACT ASSESSMENTS

Does the company have a procedure in place to deliberate the impact of a new undertaking on data security and privacy? Is it the project at risk of contravening the data subject's rights or GDPR as a whole?

DATA RETENTION

As per the principle of data minimisation, can any data held on file be disposed of? Is the wider company aware of where data may be held, and therefore liable under GDPR?

THIRD PARTIES

Does the company work with any third parties? Are they compliant? Do contracts expressly outline the limits and responsibilities of each party under GDPR?

For HR, it's especially important to point out the distinctions between personal data and sensitive personal data. The former refers to any information that can be traced to an identifiable natural human being – which includes online IDs such as social media handles and IP addresses – whereas the latter refers to any data that details sensitive personal information about the subject, e.g. racial or ethnic origin, political beliefs, trade union memberships, medical records etc. The processes for handling this data largely mimics the DPA, but sensitive personal data is now subject to a higher degree of scrutiny. Gaining consent for information of this type must satisfy at least one of a number of explicit conditions laid out in GDPR.

Ongoing compliance training is necessary to mitigate the legal, financial and reputational risks associated with falling afoul of regulatory requirements. Not only will training mean employees are aware of how GDPR requires we handle personal data, training will increase accountability throughout the organisation. Employees need to be mindful of potential compliance impacts when making decisions, particularly those involving the handling of personal data. A one-off training session won't be enough; companies will need to introduce a comprehensive, ongoing training strategy to address the changes GDPR will bring.

Erik Zilinek,
Director, Legal Services, Skillsoft

COMPLYING WITH GDPR

With the deadline fast approaching, there are clear pressures for businesses. But an accurate understanding of GDPR and it's implications will allow organisations of all types to make great strides in a relatively short amount of time.

Below are some recommendations that can help initiate steps towards compliance. It can be a long road, however, following these best practices will ensure that disruption is kept to an absolute minimum and business changes made have a lasting impact.

BEGIN RAISING AWARENESS THAT SIGNIFICANT CHANGES ARE FORTHCOMING

This may seem a glib point to make, especially considering the scale of the task that some organisations are facing, but it's important to emphasise to business leaders. The importance of this point is brought into greater focus upon discovering that many companies—particularly SMEs—are wholly unprepared for GDPR, even at this late stage.

In the early stages of a GDPR initiative the most effective thing anyone can do, irrespective of department, is begin raising awareness of the forthcoming changes. Doing so serves two functions:

- Firstly, it educates the entire organisation about procedural or operational changes that will impact roles and responsibilities;
- Secondly, it demonstrates that the company is doing all it can to communicate individual privacy rights.

Remember, GDPR asks that organisations make it evident that everything is being done to achieve the degree of security and privacy that GDPR demands. While raising awareness doesn't exactly equal consent from the data subject, it does show the company is taking GDPR seriously. In the event of an audit, communication such as this is valuable, no matter how insignificant it seems.

SUSPEND ALL NON-COMPLIANT DATA COLLECTION AND BEGIN ACQUIRING LEGITIMATE CONSENT

As discussed, 'conscious' or 'legitimate' consent is the main theme that runs through the entirety of GDPR, therefore acquiring it should be everyone's top priority. It can no longer be assumed that an organisation is gaining consent from the data subject, it must be made absolutely clear to them what's happening with their data and why. It should also be communicated that the data subject can withdraw their consent at any point, and company mechanisms should be in place to allow this to happen. This means that any old data collection methods must be suspended, not only to ensure consent is granted properly from the data subject, but also to reduce the amount of data that is incoming (as per the data minimisation principle). This task may sound labour-intensive, but it need not be. Targeted use of technology can make this process much easier.

IDENTIFY AND LOG ALL CURRENT DATA

Thorough internal audits of an organisation's current state of affairs should feature prominently on a list of priorities. Without an understanding of what data is held, you cannot begin to implement data handling and storage procedures that are genuinely effective, let alone compliant. Entire companies should be assessed to reveal the extent of personal and sensitive personal data held on file, where exactly this information is held, in what format it is held, and who has access to it. These discoveries should then be categorised and documented accordingly, with any remedial actions required being noted down.

REVIEW CURRENT DATA PRACTICES

Once organisations know what, where, and why they have the data they do, they will then need to ask themselves if current governance practices are sufficient enough to comply. In most cases, changes will be necessary to comply with the more stringent rules of GDPR.Project teams will need to review what improvements or changes need to be made to current processing practices, ensuring they remain lawful throughout the entire data flow. Internal records must be kept with any processing activities, as well as being tagged and classified. Companies will need to pay close attention to overseas movement of data, particularly outside of the EU, to ensure storage and processing remains on the right side of the law at all times. The Information Commissioners Office (ICO) has produced a data protection self-assessment toolkit (see: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/) to help organisations check their readiness for GDPR. Even those fairly confident of their position would be well-advised to carry out one these as a matter of due diligence.

CREATE OR REDESIGN COMPANY LITERATURE

GDPR is about individual empowerment and company literature should therefore reflect this. Consent cannot be properly granted under GDPR if the data subject is unaware of their full rights. Therefore, redrafting of company documents should be done if the rights of the individual are not clearly communicated throughout, and privacy statements should also be updated to reflect the changes put in place by GDPR.

APPOINT A DATA PROTECTION OFFICER (DPO)

IT and HR will have a real stake in the success of a company's new data protection practices, but GDPR by nature of its scope will implicate everyone to some degree. This means that coordination and clarity is paramount. GDPR recommeds that businesses appoint a DPO, who is well-versed in data protection law, to ensure that both controllers and processors are adhering to regulatory measures put in place by the business (some entities will be obliged to appoint a DPO due to the sensivity of the data they process). Some organisations may see this as an unnecessary appointment, but the peace of mind that a DPO provides cannot be overstated. Imagine their use in the event of a data breach, for example, let alone in avoiding one in the first place. DPOs will help guide businesses through a new and unprecedented approach to data protection (that is often complex and jargon-heavy) and also help to train and prepare staff properly. Moreover, the DPO will have a critical role in the development of coherent and effective GDPR strategy that adheres with the strict understanding of consent outlined in the regulation. In short, the technical competence that a DPO provides will ultimately benefit every organisation, no matter its size or complexity.

WHEN DO YOU NEED A DPO?

Employing a DPO is definitely a positive step towards achieving a compliant position, however only certain organisations are obliged to appoint one. This figure might not be a full time employee, but rather a paid-for service that is used when required. As such, the impact this obligation will have on certain organisations need not be costly. An entity will need to appoint a DPO when:

- The processing is carried out by a 'public authority'. This definition is not clearly defined within the regulation. GDPR suggests that this designation be defined as per national law.
- Its 'core activities' require consistent and systematic monitoring of data subjects on a 'large' scale'. These 'core activities' can be otherwise read as the functions necessary to achieve the controller and processor's goals. Again, like 'public authority', 'large scale' isn't clearly defined but this can be read as a significant and established organisation that needs to monitor personal information on a constant basis, like a bank for example.
- When these same 'core activities' involve extensive processing of sensitive personal data as defined by GDPR, such as health records, ethnic orgin, political allegiances, criminal convictions and other offences.

APPROACH ALL NEW TASKS WITH A 'PRIVACY BY DESIGN' ETHOS

Companies regularly embark on new projects that will require new information from their employees or members of the public. These projects should here onwards be approached with a 'privacy by design' ethos. This may mean having to alter established methods that have produced results in the past, but the time saved being compliant from the very beginning will pay off in the long run. Imagine having to backtrack through months of work to ensure consent was adequately granted and processing is compliant. This will cause frustration and potentially thousands of hours of wasted labour. Getting it right first time makes sense.

TEST AND UPDATE NETWORK SECURITY AND ESTABLISH BREACH REPORTING MECHANISMS

The introduction of GDPR should be viewed as an opportunity to assess the effectiveness of network security. This is mostly the remit of IT professionals, but all employees can play a role in ensuring data integrity by 'stress-testing' company assets like the website and protection measures such as firewalls. At this stage, companies should also be thinking about their breach reporting mechanisms in the event of a serious failure, paying particular attention to how and when affected individuals are notified. This point, and the previous one, can also be considered on a cultural level. Companies can improve standards by promoting a 'data secure' mindset in day to day office activity, e.g. asking every employee to lock their computers when not manned, or requesting they consider the physical documents they leave out on desks.

DON'T FORGET ABOUT THE HIDDEN RISKS

The severity of penalties might blindside companies into focusing too much on their own procedures without considering their relationships with third parties or contractors. Discussions should be had to ensure all parties are compliant and contracts should be reviewed so that responsibilities are explicitly detailed and understood. With GDPR being very much a digital regulation, these same organisations may also forget about the physical historical data that is hiding in their archives. Paper-based filing should not be forgotten about, nor should the potential non-compliance of business partners. Be thorough to be sure.

EMBRACE CHANGE

The consequences are now too severe for organisations to take anything other than a highly judicious approach to data protection and privacy. But the fines shouldn't be the only thing that crosses management's mind when implementing changes resulting from GDPR. The new law is there to both protect businesses and individuals from unnecessary risk. It's ultimately for the greater good. Businesses should therefore be embracing the opportunity to improve their practices and put employees' rights at the centre of their operations—it ultimately reflects well on the organisation. Remember, big changes to data protection only need to be made once and from thereon only minor adjustments.

WHY DOES GDPR BENEFIT ORGANISATIONS?

Conservative estimates place the number of connected devices expected to be in circulation by 2025 at 75.44 billion, clearly there is a need for laws that harness this staggering growth and accompanying risk to data security. This isn't just a nominal change by overzealous regulators, it's a vital step in the right direction. But how does it benefit organisations?

Firstly, GDPR aims to bring basic human rights of privacy and security front and centre—a motion few organisations could argue with. The new regulation will also oblige businesses to take data protection far more seriously than ever before, primarily because their reputation will rely on it (and the penalties are crippling even for hugely profitable companies). Research shows that customers are more likely to choose a different company if they feel their data will be at risk of falling into the wrong hands. Through the improvements of GDPR, customers will be more willing to work with a company safe in the knowledge that their data and privacy is considered a top priority. The fear of a very public-breach (and the ensuing penalties) will force the hand of even the most negligent organisation. This effect will inevitably see data protection standards improve across all sectors – not to mention across the globe due to the extraterritorial effect that was explained earlier.

Organisations should view GDPR as an opportunity to get their data security in order and a change to improve their brand reputation. Many companies will be motivated to make the data security a top priority as a result of GDPR and will adopt secure data handling practices. When data is handled in a transparent and secure process, organisations can use this as a competitive advantage in the future.

Craig Fearon,
Senior Principal, Product Management, SumTotal Systems

In short, GDPR is not simply 'red tape' for companies to traverse, but rather an opportunity to effect lasting positive change that sees both brand loyalty and consumer confidence drastically improve.

On a more practical level, GDPR will bring some cost savings and improved efficiencies. The regulation will force companies to address archives of data and ask whether that information is truly necessary or fit for purpose. Data maintenance will therefore become a more 'active' process that is managed regularly, rather than every so often which often sees long disruption to operations as a company is assessed 'in-depth' (a labour-intensive and therefore costly procedure). The GDPR will also see organisations assessing the efficacy of their networks and technology, with many having to migrate over to improved infrastructure. This move will enable companies to align better with the latest and emerging generations of technology as old hardware is replaced with more capable (and secure) devices. While this will be initially expensive, it will be offset through an improved user-experience for employees that will promote greater levels of engagement and productivity.

But GDPR not only looks to empower the public, it also wants to improve trust in the emerging digital economy. By streamlining data protection across the EU (and effectively the world), goods and services will flow more freely, and confidence between organisations and the public will increase. In turn, this is expected to translate into greater prosperity, securing the future for a portion of the economy that only expected to grow in importance as time passes. Data protection for an increasingly digital world – it makes sense for everyone.

Pairing Skillsoft Compliance Solutions with SumTotal's Talent Expansion Suite allows organizations to easily train employees to comply with regulations such as the General Data Privacy Regulation (GDPR). Skillsoft's GDPR compliance training course helps employees understand their responsibilities in mitigating the risks surrounding this upcoming regulation. The Skillsoft and SumTotal solution provides organisations with the necessary technology and training to manage their compliance obligations within an ever-evolving regulatory landscape.

ABOUT SKILLSOFT

Skillsoft is the global leader in corporate learning, providing the most engaging learner experience and high-quality content. We are trusted by the world's leading organisations, including 65 percent of the Fortune 500. Our mission is to build beautiful technology and engaging content that drives business impact for today's modern enterprise. Our 500,000+ multi-modal courses, videos, authoritative content chapters and micro-learning modules are accessed more than 130 million times every month, in 160 countries and 29 languages. With 100 percent secure cloud access, from any device, whenever, wherever.

www.skillsoft.com

ABOUT SUMTOTAL SYSTEMS

SumTotal Systems, LLC, a Skillsoft Group Company, is the world's only Learning, Talent, and Workforce Management integrated system. SumTotal's award-winning Talent Expansion Suite enables organizations to discover, develop and unleash the hidden potential within their workforce and entire business ecosystem. SumTotal goes beyond traditional talent management and HCM applications, offering contextual and pervasive HR solutions that help improve employee performance in real time.

www.sumtotalsystems.com

ABOUT HRREVIEW

HRreview is the UK's leading independent HR news, information, opinion and analysis resource dedicated to human resources and related professionals.

www.hrreview.co.uk

HR review