KASPERSKY lab

Fighting fit: running rings around GDPR compliance

There's no escaping it – the General Data Protection Regulation (GDPR) is coming and no matter what part of a business you work in, be it HR or marketing, legal or IT, it will affect you and have an impact on your working day. If you handle, hold or use personal data – whether it's employee details, customer or prospect information – GDPR will bring change to your working practices and it's up to you to make them.

Bearing the burden of GDPR

"Adhering to data privacy regulation is nothing new for companies based in the EU."

Much like a personal trainer gives you the motivation and structure to succeed, this guide will set out a plan of attack, to help cut through the noise and get you over the line to achieve your GDPR goal of becoming compliant.

Adhering to data privacy regulation is nothing new for companies based in the EU. But when GDPR is enforced on 25 May 2018 – replacing the Data Protection Directive 95/46/EC – they will need to be ready to cope with a new approach to data privacy, which empowers EU citizens to have more control over their personal data and what happens to it.

With much of the hype and focus to date firmly on the readiness of companies across Europe to meet the new criteria – and the associated fines if they don't comply-what does it all mean for individuals within a company and is the burden they face bearable?

Despite these key changes, much of the ground work has already been done under existing data protection regulations. Far from being a burden, the stringent nature of GDPR is a good thing for businesses and can have untold benefits for the future health and well-being of their organisation if approached in the right way.

Whilst those above you might have the wheels in motion for dealing with the bigger picture, each employee needs to be up to the challenge of getting the health of their data in order. The security and safe keeping of data in your possession will become of even more importance. With the goal and objectives of GDPR firmly set, it's up to the entire business to pull together to reach this key compliance milestone and streamline their data management practices across the board.

Much like tackling a change in lifestyle or objective to get fit and healthy for the summer months, approaching GDPR at a departmental level can only be achieved by making small, but significant changes which all come together to ensure you are fighting fit for when GDPR enters the ring in 2018.

Before we can break down the challenge ahead, it's important to understand the key changes[1] that will affect you:

- All personal data you control and manage – regardless of whether the processing takes place in the EU or not – will need to be processed fairly and transparently, with clear usage given to the data subjects (i.e. citizens).
- Severe financial penalties will apply for breach of regulations – up to 4% of annual global turnover or up to €20 million (whichever is greater).
- Stricter consent will be needed for data usage, making it just as easy for citizens to withdraw consent should they request it.
- Data breaches must be notified within 72 hours of the data controller becoming aware.
- Data subjects will have improved rights to obtain confirmation about how, where and for what purpose their data is being processed.
- Data erasure (or "the right to be forgotten") will be made easier, with data subjects able to request that their personal data be erased or processing stopped (providing their request meets certain conditions).
- Data portability will be enabled, giving data subjects the right to receive personal data concerning them.
- Data protection processes (or "privacy by design") must be included from the outset of designing new systems, rather than an add-on later.
- Data protection officers will become mandatory for those whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or in some cases where companies are processing significant volumes of 'special category' data.

1 http://www.eugdpr.org/key-changes.html

The sales and marketing migraine

"Isn't GDPR only going to slow us down and add to the red tape of getting our email campaigns and sales team in front of the right people?"

Departmental data detox:

- So where do you start? Instead of taking a knee-jerk reaction or "binge diet" approach to dealing with your data dilemma, if tackled in the right way, achieving long term data health and GDPR compliance can be easier than it seems.
- Bite sized, achievable health and fitness plans with clear goals and milestones will ensure every department is fighting fit to combat anything GDPR throws at them, and help steer the business towards long-term data health with no chinks in the armour or weak parties bringing it down.

Common complaints

The sales and marketing machine is typically focused on using customer and prospect data to drive sales leads and enhance brand awareness. With vast databases and targeted campaigns, the department already has to adhere to strict data protection guidelines and operates an opt-out policy to ensure compliance.

The GDPR effect

If you use personal data to deliver targeted marketing and sales campaigns, then you must adhere to the updated regulations. Relying on pre-ticked boxes on forms, or marketing to people who haven't specifically unsubscribed will no longer constitute consent. Explicit, opt-in consent is required for processing sensitive personal data, however for non-sensitive data "unambiguous" consent is valid. Provision for deletion of data also needs to be made under "the right to be forgotten", which will make it easier for individuals to ask for their information to be removed from your database.

Your five-step data fitness plan

- Opt-outs, or those who remain silent, must now opt-in or give explicit consent in some way if you want to keep them on your marketing hit list. But before you trawl through your entire database, think about the best way to enable this to happen to give you a valuable and cleansed marketing list as a result.
- Your database needs to opt-in and respond, so give them a reason to do so with a strong call to action and compelling content.
- Under the terms of GDPR, consent text accompanying marketing material needs to be clear and concise, making it easy for people to make a decision about if and how you can use their data.
- Keep a clear audit trail and record of who has opted-in.
- You need explicit consent to market to an individual – attendance at an event or business card left at a trade show is not sufficient to add them to your marketing mailer database. They either need to explicitly untick a box to show clear, affirmative action or actively provide another statement or action which clearly indicates the data subject's acceptance of the processing or their personal data. This could include providing their email address in an optional section in an online form, which has a supporting disclaimer about its usage.

The legal low

"Ensuring our staff understand and stick to the rules and that our contracts and supplier SLAs meet GDPR compliance, is going to put a huge strain on our resources."

Only 38%
of IT decision makers have a good knowledge of GDPR

Common complaints

The legal team already has to deal with a raft of regulations to ensure the company adheres to data privacy and protection laws and they would be forgiven for dreading the impact of GDPR on their day to day roles.

The GDPR effect

Not everything needs to fall on the shoulders of the legal department. However, there are key areas which they need to address. Managing contracts and negotiating with clients and suppliers is one such area. Under GDPR, your business will be liable for any breach of rules associated with the data processed either in-house of via a third party or through partners you work with, so ensuring compliance across the board is vital. From your internal teams and marketing database, to your PR agency and outsourced data centre: if rules are not followed or a breach occurs, it will have a significant impact on your business. Ensuring you have robust data safeguarding policies in place is paramount.

Your five-step data fitness plan

- Any contracts which extend beyond the GDPR deadline, will need to be reviewed and updated as necessary, to ensure they meet the new data processing regulations.
- Ensure that any new contracts or negotiations take GDPR into account, to save last minute panic a year down the line when things need to be changed.
- This can be done by adding in specific clauses which mean they can be easily amended to comply with GDPR when it comes into effect.
- To make this easier when the time comes, signpost when these changes need to happen in project plans or timelines.
- Work with your suppliers to ensure compliance. The regulations affect them too and by working together you can maximise resources and ensure a robust response on both sides, so that all parties know what their responsibilities are should a breach happen or data subject make a request about their data.

The finance and accounting Achilles heel

32%

of IT decision makers have minimal or no awareness that EU businesses must report a data breach within 72 hours under GDPR

"GDPR is going to have a huge impact on the way we work, with even more eyes on our department to ensure we are processing and securing data to the letter of the law."

Common complaints

The finance function is a highly-regulated area and already firmly in the accountability firing line, processing vast amounts of sensitive and personal information every day.

The GDPR effect

Due to the volume of personal data they work with, the finance and accounting function will become a big focus for the data protection officer and the regulators who are tasked with ensuring GDPR compliance. The security of personal information moving across their systems is where the big fines can come, if any breach occurs. But, with the function already used to operating under strict regulatory controls, GDPR will only help to strengthen the robust and transparent nature of the finance function.

Your five-step data fitness plan

- Ensure there is a clear escalation process in place within the department to immediately report any data breaches to the authorities, should the worst happen.
- A data audit will assess what changes you need to make to current practices to ensure compliance. This won't mean starting again with policies but updating them to ensure you tick the new GDPR boxes.
- Automating processes will help to reduce human error and reduce the risks associated with the data breaches – whether intentional or unintentional.
- Review data storage procedures which cover the retention and destruction of personal records, as the parameters will change under GDPR.
- Put data protection at the heart of all processes moving forward and don't think of it as an add-on, but a core part of doing business.

The HR headache

29%

of IT decision makers have minimal or no awareness that the regulations apply to EU personal data stored inside and outside of Europe

"With storage, safeguarding and deletion of HR data already a cumbersome task and regulatory headache, surely GDPR will only bring the department more pain?"

Common complaints

HR holds a great deal of personal data – from CVs of existing and former staff, as well as unsuccessful candidates, through to employee data including contact and banking details.

The GDPR effect

Under GDPR, employees will have enhanced rights over the use and retention of their data, giving employers a potential headache. But whilst the impact upon HR is significant, the challenge is not insurmountable. The department will need to be more transparent about their intention for the personal data and provide the ability for employees to request it be suppressed. This applies to current and former employees.

Your five-step data fitness plan

- To relieve pressure on HR, an audit of current data handling processes and policies is the first logical step to understand where any changes need to be made.
- This will help ascertain where updates need to be made to employee contracts, handbooks and company policies.
- Empower those in your team by providing more information to employees and job applicants on the purpose and legal grounds for collecting their data and ensuring they know their rights.
- For prompt response to a data breach, nominate a response individual or team to react to any incident.
- Regular training in how to identify and respond to a breach coupled with appropriate policies will ensure this aspect of the regulation is tackled calmly and with confidence.

The IT irritation

" My remit doesn't include holding or managing personal data, so why should I care about GDPR?"

22%

of IT decision makers are not confident that their organisation will be fully compliant with GDPR by May 25 2018

Common complaints

For IT professionals, keeping the company's infrastructure running and systems robust and reliable is their number one challenge. GDPR is not something that is explicitly on their radar. However, effective IT processes underpin the very fabric of ensuring and maintaining GDPR compliance and achieving a streamlined, secure and transparent approach.

The GDPR effect

GDPR will affect the IT department in a variety of ways and cross over with other departments, as they update and streamline their processes. For example, the marketing team will require support for their opt-in and email campaigns, to ensure the technology is there to keep track of consent forms etc. With greater onus on citizens being able to access their information and have it removed or to have a better understanding of what it is used for, systems and programs which hold this information must be easy to navigate and ensure complete transparency for those using them. Securing the data held by your organisation is also vital.

Your five-step data fitness plan

- Work with other departments in the organisation to understand their needs and how it affects the software and systems they use and what support they need in order to comply with GDPR.
- Catalogue every piece of personal data to ensure transparency and easy access to information as needed for reporting purposes or to fulfill data subject requests.
- Set up clear audit trails for every piece of personal data moving in and out of the organisation.
- Apply privacy specific measures to safeguard information and minimise the likelihood and impact of data breaches, including encryption and anonymization.
- Address GDPR requirements at the planning stage of any new software or infrastructure updates, to ensure it complies and that data is secure and integrity maintained.

As much as 17%
of IT decision makers say their organisation has made little or no preparations for GDPR

Call to action: Group exercises

The task ahead might look daunting, but businesses and individual departments are already making good progress in getting their data health in order. To help get them over the line and keep the business running at peak condition, habits towards the security of personal data need to be strengthened and maintained across the board.

Your five-step data fitness plan

- **Go the distance** – There is no long-term reward in taking a half-hearted approach to getting your business GDPR-ready. Future proofing new procedures is key. It could cripple your business if the right steps are not taken now.
- **Nominate a coach** – Each department needs someone to bring it all together and keep everyone on track and to plan.
- **Clear your mind** – Achieving departmental and organisation change requires an open mind and willingness to change processes for the long-term health of the business.
- **Train regularly** – Data protection policies need to be regularly updated and clearly communicated to all departments, staff and suppliers.
- **Work with a personal trainer** – Third party support will not only help you to stay on track but help you maintain good data health moving forward.

Unless stated, all statistics included in this whitepaper are taken from research conducted for Kaspersky Lab by Arlington Research in April 2017. Over 2,300 IT decision makers from across Europe, within companies of 50 or more employees, were questioned about their views and awareness of GDPR.

For more information about Kaspersky products and services contact your account rep or visit www.kaspersky.com

Kaspersky Lab
Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK
www.kaspersky.com