The Essential Guide to GDPR Compliance

Get regulation ready with HP

Brought to you by hp

Contents

Introduction

It’s time to adopt privacy by design

On 25th May 2018, the EU’s General Data Protection Regulation comes into force. It will replace every national data protection regulation within the EU, and anyone who does business within the single market will have to comply with it. That includes non-EU businesses who deal with EU customers.

Under GDPR, any breach of personal data must be reported within 72 hours of awareness. Failure to do so – or to disprove negligence – can result in fines of up to €20million or 4% of global turnover, whichever is higher.

Fortunately, the measures required to protect the company’s data as a whole will also serve to keep customer’s data safe. The same multi-layered endpoint security approach we at HP already recommend will help to ensure compliance with GDPR.

In this eguide, we will examine the key components of GDPR that IT professionals need to know, and look at how a device-led, endpoint security program can help with compliance.

EU GDPR explained

The key points for IT

There are essentially two aspects to the GDPR: protecting the rights of EU data subjects and protecting the privacy of EU data subjects. Both have technological implications.

For the authoritative detail, read the full text. But for IT decision makers, these are the points you need to know:

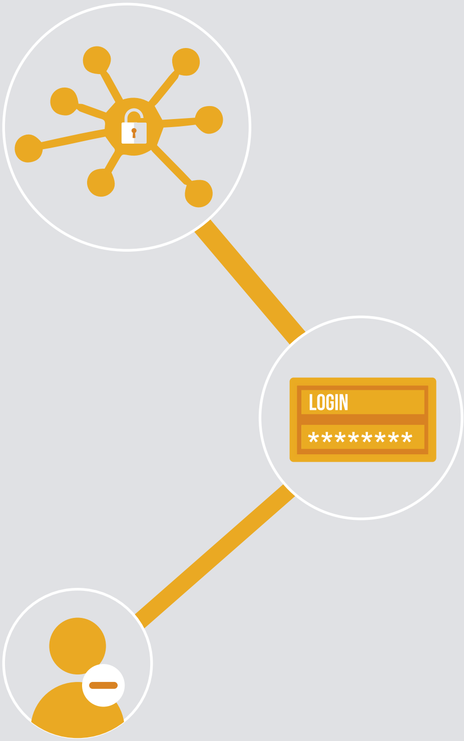
1. **Breaches must be reported within 72 hours**
   Should a data breach occur, it must be reported within 72 hours of awareness. The penalties for failure to do so are steep (see p5 'What are the penalties for non-compliance?')

2. **The right to be forgotten**
   Every EU data subject has the right to be forgotten. Upon request, you must erase their data including all copies

3. **The right to data portability**
   EU residents have the right to control their own data. Upon request, you must provide their data in a format accessible to them, that they are permitted to transfer to a third party

4. **International transfers**
   Moving personal data to another data jurisdiction (i.e. outside of the EU) can only be done with explicit consent, and only to regulators deemed 'adequate', or with additional safeguards put in place[1]

5. **Privacy by design**
   Organisations must adopt a privacy by design approach that integrates data security into products, processes and services by default[2,3]



Who does the GDPR apply to?

The GDPR applies to any company collecting and/or processing the personal data of EU residents. This includes organisations based outside of the EU that operate within it.

[1] https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2] Allen & Overy – The EU General Data Protection Regulation 2016
[3] http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

EU GDPR explained

What counts as ‘personal data’?

Under the GDPR, ‘personal data’ includes “any data that can be used to identify an individual.”

This includes genetic, mental, cultural, economic or social information, alongside that traditionally considered to be identifying information.

This may bring organisations previously outside of the scope of data protection legislation under the purview of the GDPR.

What are the penalties for non-compliance?

The maximum fine is €20million or 4% of global turnover, whichever is higher. This is for the most serious offences under the regulation, such as failure to report a security breach within 72 hours of awareness.

Less serious offences attract a maximum of €10million or 2% of global turnover. Needless to say, the costs of non-compliance are significant.

GDPR procedure checklist

Within your Data Governance framework, you will need explicit procedures for:

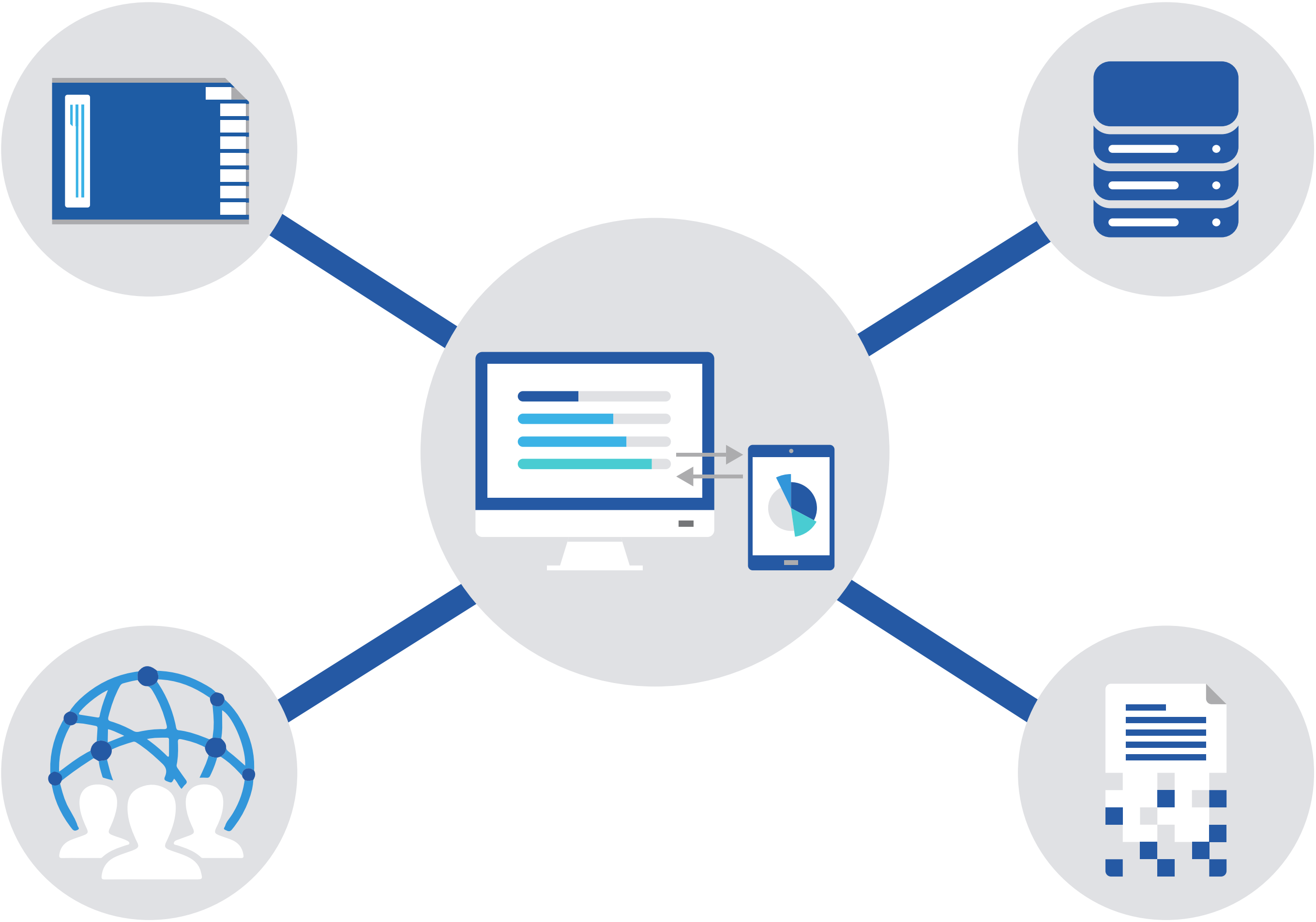
- Informing data subjects of how their data will be gathered, stored and processed
- Obtaining data subjects’ explicit consent to do so
- Providing data subjects’ information in a format accessible to them
- Erasing all of a data subject’s personal data, including copies
- Transferring data to another data controller or processor
- Transferring data outside of the EU – including within the organisation

Technical challenges to compliance

The biggest challenges of GDPR are technical.

Enabling secure data portability, protecting individual's data and their right to be forgotten requires a comprehensive map of data location and access down to device level.

As the threat from cyber crime increases year-on-year maintaining absolute security is a growing challenge.



Technical challenges to compliance

Keeping track of devices

Complying with data portability and the right to be forgotten requires a detailed account of all personal data held by the organisation.

You need to know:

- Every device that holds personal data
- Every device that has access to personal data

This is the only way to guarantee you can retrieve and/or erase personal data held by the company.

Keeping track of clouds

The average European enterprise uses 608 apps, a figure estimated as 90% under-reported. Employees often use commercial cloud apps without the IT department's knowledge.[4]

For GDPR compliance, cloud use must be confined to services that are:

- Within the EU, and therefore GDPR compliant themselves
- Under the jurisdiction of a data protection regulator deemed 'adequate' by the EU

Anything else could breach the international transfer rule. And you need to know what cloud services employees use, should the right to be forgotten be invoked.

Keeping data defended

The threat for cyber crime is growing. Not least because use of unsecure networks and personal devices is growing too.

Breaches are nearly inevitable. The EU knows this. But to avoid a costly fine you must:

- Implement a Systems Incident Event Monitoring (SIEM) tool to report a breach within 72 hours
- Implement multi-layered endpoint security to demonstrate due diligence in preventing a breach

Users must also be made aware of their responsibilities in not using unsanctioned devices and networks.

[4] https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

The threat from cyber crime

Cyber crime is a real, present and growing threat

82%

of organisations have experienced a threat/ breach within 12 months[5]

80%

of IT professionals think the cyber crime threat will increase in the next three years[6]

78%

of businesses report an increase in malware attacks over the past five years[7]

60%

of IT leaders feel cyber crime is outstripping defences[8]

81%

of businesses rate insider negligence as the biggest threat to cyber security[9]

81%

of IT leaders say mobile devices on their network have been a target for malware[9]

72%

say employee use of commercial cloud software is a risk[9]

69%

say BYOD is a security risk

[5] HPI Printer Security Research 2016 (Spiceworks) [6] HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8] IBM CISO Assessment 2014 [9] Ponemon 2016 State of the Endpoint Report

Implementing endpoint security

HP's multi-layer approach to endpoint security

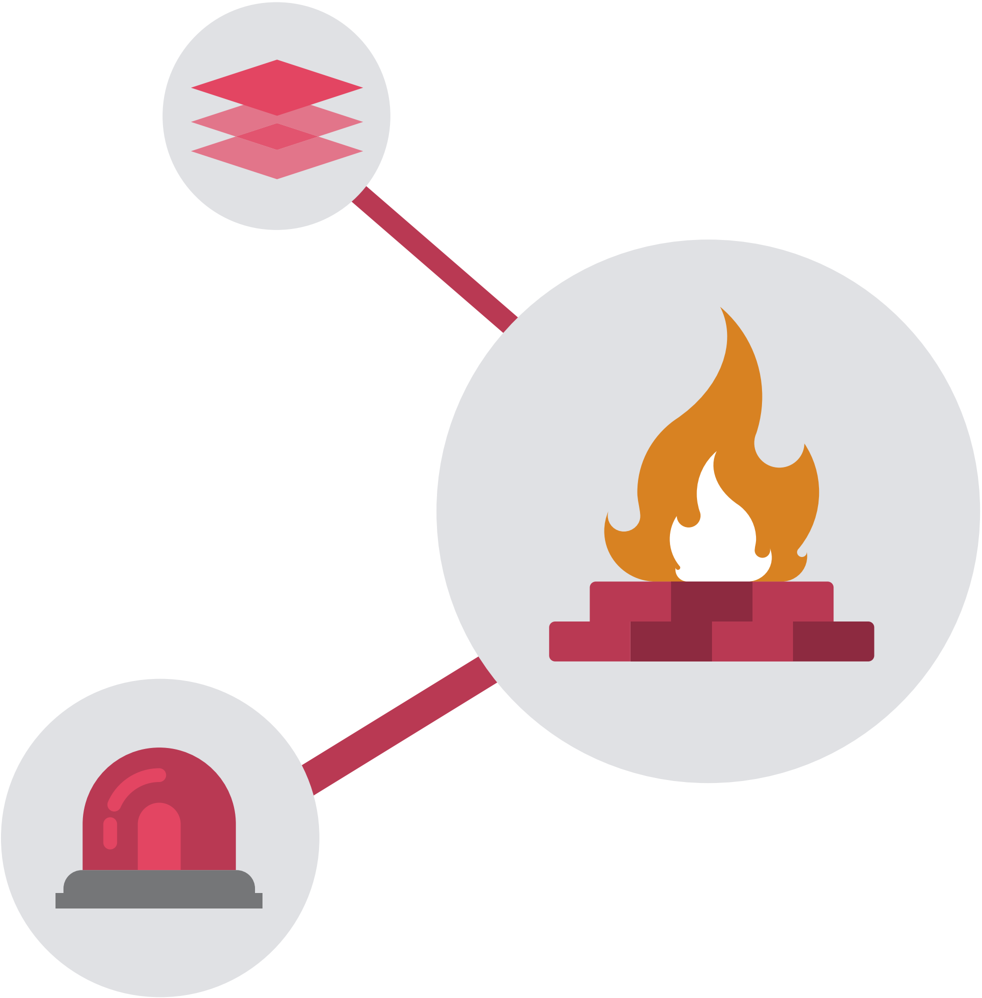
The prevent and protect approach to cyber security – firewall and antivirus - is not enough. It never was. In a study by Damballa, antivirus software took six months to identify and eliminate 100% of malicious files thrown at it.[10]

HP's view is that cyber security must be multi-layered, operating at network, device and user level, with multiple defences on each. Detect and respond should be favoured over protect and defend. And the endpoints are the starting point: both device and user.

Critical Security Controls (CSC)

The Center for Internet Security (CIS) has defined 20 internationally recognised Critical Security Controls (CSC) developed, refined and validated by leading IT security experts around the world. These are seen as important cyber hygiene actions for every organisation.

We've made reference to the key CSCs for GDPR compliance as they are useful guidelines, but the full text is available online. Download it for free at the CIS library.



[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Network security

Major hacks tend to exploit a single point of entry to gain access to the entire network. Network-level security should therefore be based on preventing that.

- **Control administrative privileges (CSC 5)**
  Restrict ability to change network settings and passwords to as few people as possible

- **Control access based on need to know (CSC 14)**
  Tier access to sensitive information on user, device and location. Weigh security risk against sensitivity of data

- **Limitation and control of network ports, protocols and services (CSC 9)**
  Switch off any unnecessary access points – virtual and physical - including FTP, Telnet and print services

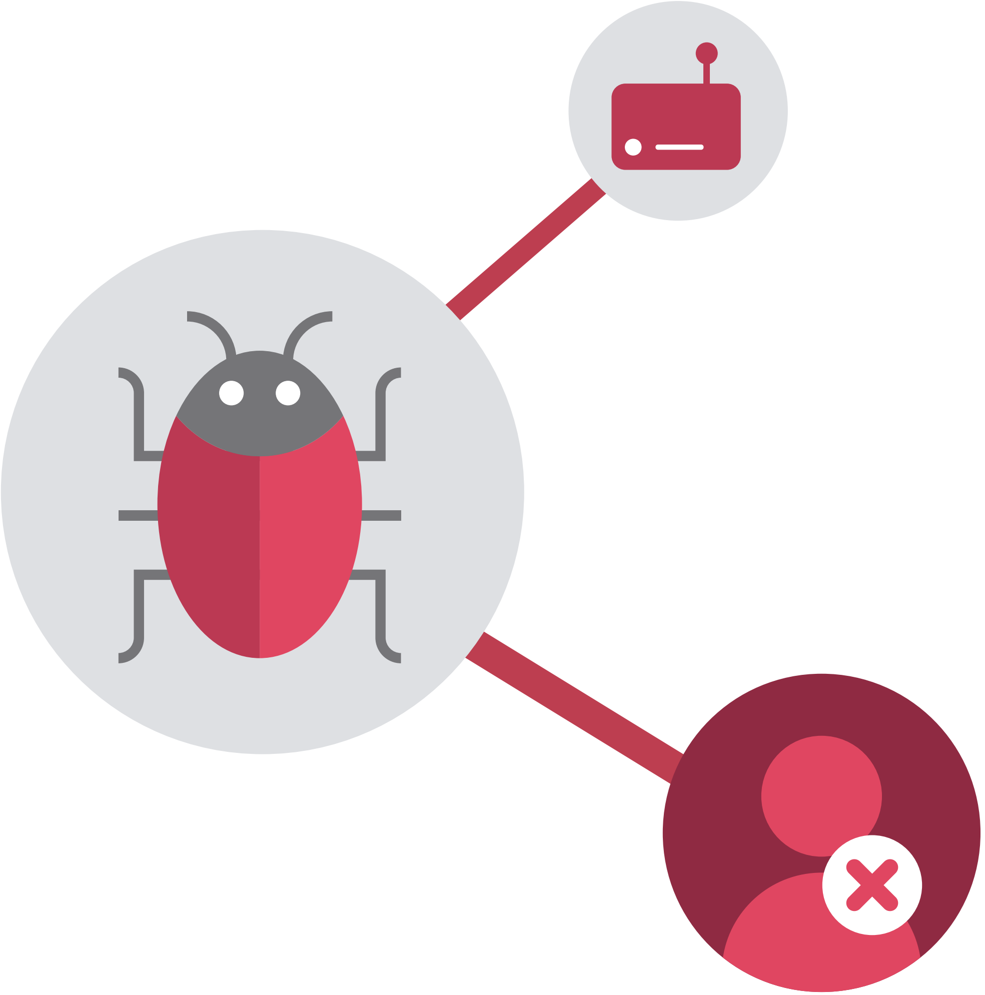
- **Maintenance, monitoring and analysis of audit logs (CSC 6)**
  Regularly review audit logs to analyse system behaviour and detect any suspicious activity

- **Continuous vulnerability Assessment and Remediation (CSC 4)**
  Continuously assess the environment for vulnerability and take action to remediate on results, minimizing opportunity for breaches

The goal is a network subdivided according to sensitivity of information. Access requests are evaluated for security risks. Unrecognised devices, users and requests from unsecure networks are blocked from the most sensitive information. Google's BeyondCorp policy is a good model.[11]

[11] https://research.google.com/pubs/pub43231.html

Network security



Every device is a potential vulnerability, whether business or personal. You need to know every phone, tablet, laptop and desktop that has access to company data.

- **Inventory of authorised and unauthorised devices (CSC 1)** Audit every device that has access to data
- **Inventory of authorised and unauthorised software (CSC 2)** Audit every application used on the network – to directly access data or not
- **Malware defences (CSC 8)** Ensure every device has up to-date antivirus and malware. Ensure regular scans and updates

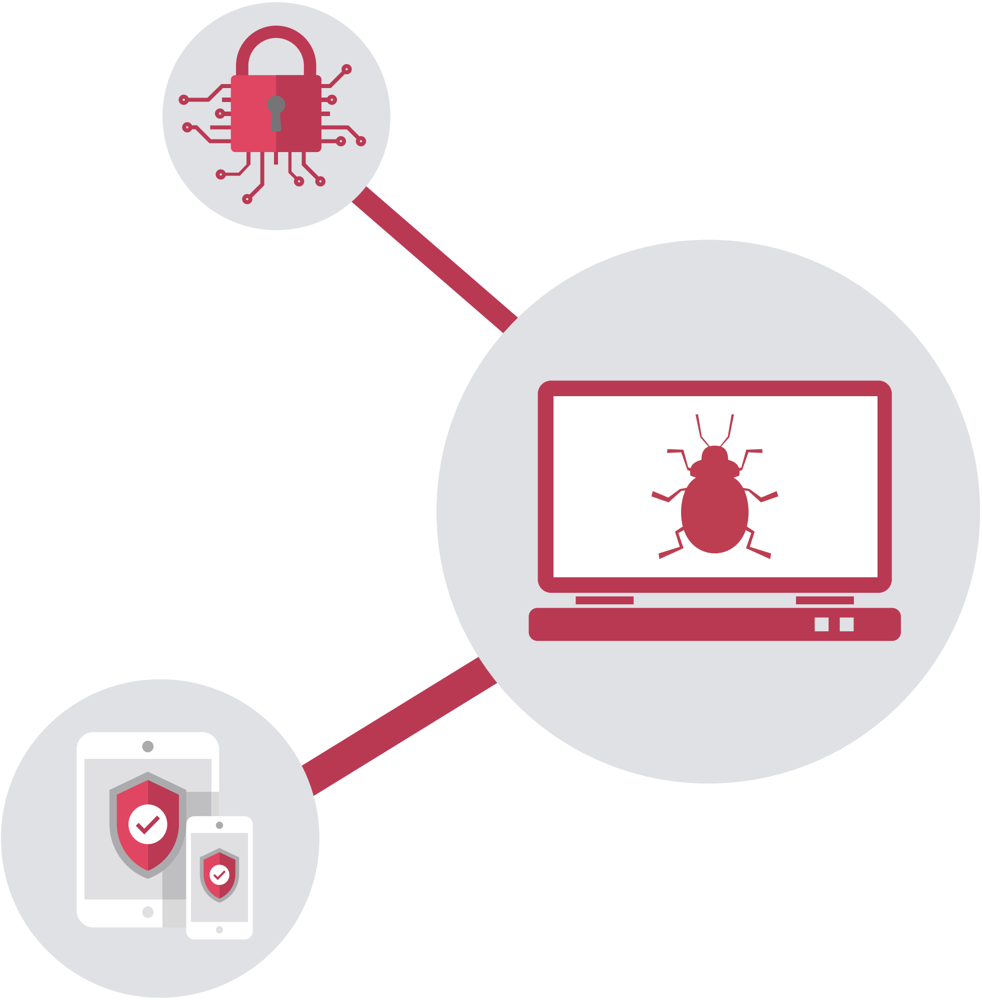
Device security

In addition IT departments should consider these additional checks:

- **Multi-factor authentication**
  Ensure every work device is secure. Ideally, use biometric authentication alongside passwords (see p14 'Privacy by design devices')
- **Remote access**
  Ensure remote device access to retrieve or erase personal data, quarantine and terminate processes, and shut down and lock the device in the event of loss or theft (see p14 'Detect and respond')
- **Inform every employee of security protocols and procedures**
  Ensure every employee is aware of, and knows their responsibilities regarding cyber security, including flagging suspicious activity
- **Run active cyber security training**
  Host workshops, seminars, run phishing drills – ensure everyone knows how to avoid basic mistakes, and how to remain GDPR compliant
- **Minimise personal device/app use**
  Discourage use of personal devices and apps for work purposes. A comprehensive and flexible CYOD policy should help

Implementing a security framework like this, should help you in maintaining control over company devices, to help protect data and facilitate the enforcement of data portability and the right to be forgotten.

For more on HP's approach to multi-layer security, read our whitepaper, Security Begins at the Endpoint.



Why every employee needs to be cyber aware

58% of cyber threats come from employees, ex-employees and trusted partners.[12] Securing every device means securing its user too.

- The U.S. Democratic National Committee (DNC) was hacked in 2016 when John Podesta clicked on a phishing link mistakenly flagged as legitimate by an aide[13]
- Nude celebrity photos flooded the internet in 2014 after 36 year old Ryan Collins gained access to Jennifer Lawrence et al's iClouds with basic phishing emails posing as Apple[14]
- 68m Dropbox passwords were leaked in 2012 thanks to an employee using the same password for internal systems as for his LinkedIn[15]
- President Donald Trump continues to use a standard Samsung Galaxy phone. Experts don't wonder if it's been hacked, rather how many foreign intelligence agencies have already[16]

[12] http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13] https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14] http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16] https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Detect and respond

Detect and respond is a cyber security framework that recognises that total prevention is near-impossible.

What matters is becoming aware of the breach (detect) and taking immediate action (respond).

Software products are available that turn each device into a real-time sensor, and that allow the administrator to respond by e.g. shutting down devices, quarantining files and erasing data.

Privacy by design devices

HP's devices embody privacy by design.

Security features include the world's first self-healing BIOS, automatic Bluetooth lock – that locks the device when you walk away – and integrated privacy screens.

These features won't ensure GDPR compliance by themselves, but they'll certainly help.

Preparing for GDPR

Practical steps to take now

The GDPR comes into effect on May 25th 2018. There's still time to get prepared, but as you're no doubt aware by now, there's plenty to do.

The first step is to **audit your current data situation**. Assess where your data is stored, where it gets copied to and who has access to it. If you use any cloud solutions, find out where their servers are based and if they will be GDPR compliant. The same goes for any SaaS or other partner organisations you work and share your data with. This will give you a clear idea of how much needs to change in order to comply

Design your data policy. Include detailed procedures and protocols on where data is stored, who has access and making copies outside of the company, or across borders within a multinational. Include procedures for retrieving and erasing personal data. Communicate this to everyone in the company. Run training sessions. Underline its importance.

Design your security policy. Create a new cyber security framework that works from a detect and respond endpoint basis. Overhaul your device policy if required. Invest in new technology if required. Only 36% of IT leaders feel they have enough budget for endpoint security.[17] The GDPR penalties may finally be the stick to get the C-suite interested.

[17] Ponemon 2016 State of the Endpoint Report

Preparing for GDPR

GDPR checklist

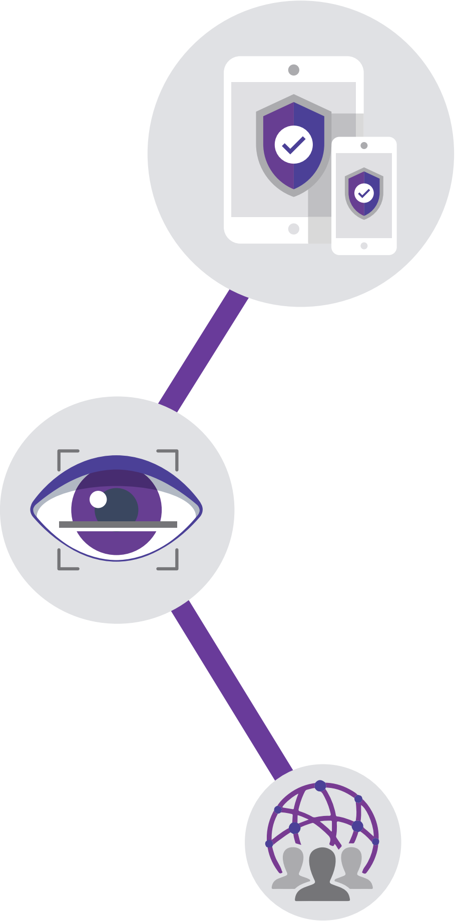
5 key steps towards GDPR compliance

1. Appoint someone to be in charge of data, a Data Protection Officer (DPO) if required
2. Conduct a full data audit, including suitability of cloud and SaaS providers with reference to GDPR
3. Create a new data governance framework, including procedures for data portability and right to be forgotten
4. Create a new cyber security framework, implementing multi-layered endpoint security
5. Communicate policies and protocols to everyone in the company

Device Security Checklist

6 key steps to securing endpoints

1. Audit all authorised and unauthorised devices with access to personal data
2. Invest in new – more secure – devices if necessary
3. Implement remote access and erasure rights for company data on devices
4. Implement a regular scan and security software update policy
5. Implement real-time detect and response software
6. Train employees in cyber security



Endpoint security calendar

A basic timeline for endpoint security implementation by GDPR

2017

May

Appoint project manager in charge of implementing endpoint security

June

Conduct audit of current security policies, practice and devices

July

Consider device requirements & policy for endpoint security (CYOD/BYOD etc.)

August

Consider software solutions for detect and respond security

September

Design multi-layered, tiered access system for company data

October

Design public/private cloud to enable appropriate offsite data access

November

Design user training programme incl. regular phishing drills

December

Communicate new security policies to the rest of the company

2018

January

Implement new data architecture on public/private cloud

February

Implement new device policy

March

Implement detect and respond software solution

April

Conduct user security training incl. policies related to GDPR

May

GDPR comes into force

Summary

GDPR isn't far away

If you're lucky, your organisation is already practising much of what is contained in the regulations – it is, in large part, merely an encapsulation of what constitutes best practice.

And if you've been operating in multiple EU countries, you may have already encountered some of the more severe measures contained.

The security measures we recommend putting in place in order to comply with GDPR are measures that help prevent any breach, which can be incredibly costly to an organisation. At last count, the UK government estimated British businesses lost £21bn in a single year, a figure it expects to grow.[18]

Further, many of the measures required for truly robust security will also help to comply with other aspects of the GDPR. Restricting data access to particular users, devices and networks not only minimises data risk, it makes it easier to track personal data – and therefore to comply with data portability and the right to be forgotten; not to mention international transfers.

This eguide is only the beginning. Security has always been a priority at HP. Privacy by design has been our policy for years. Now that it's required, rather than desired, we are well placed to help you adopt the same approach.

To find out more about how HP and our products can help you comply with GDPR, visit **our Privacy by Design page**

[18] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf