General Data Protection Regulation

Compliance for smaller businesses working in the cloud

kaspersky BRING ON THE FUTURE

What is GDPR?

GDPR stands for the General Data Protection Regulation. It's a regulation that's been implemented in all local privacy laws across the entire EU and EEA region.

It applies to all businesses processing and storing personal data in Europe and to businesses in other countries worldwide, which provide the services to the European citizens.

'A key principle of... GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle''.

ICO Guide to GDPR — Security

The challenges

Every business, no matter how large or small, has to comply with data regulation laws. But while large corporations can afford to hire top specialists and purchase the most sophisticated tools, things are much tougher for smaller businesses looking to meet basic requirements as simply and cost effectively as possible. And there's little room for error: failure to comply can lead to huge fines.[1]

So you're doing your best to find a suitable, affordable solution. But many of the tools you need may already be part of your antivirus/ endpoint protection software, as is the case with Kaspersky Endpoint Security Cloud[2].

At Kaspersky, we've developed a stream of beyond antivirus capabilities for all your IT security needs in one security product, giving you the tools you need to keep GDPR compliant.

The requirements and how to meet them

Let's take a look at some of the things you need to do in order to ensure the compliance with GDPR, and how our cloud solution can help.

GDPR Article 28 'Processor'[3]

Article 28 sets out the requirements for the use of contractors (processors) in data processing.

Do you know exactly what external resources your employees are using to process and store data? Can these resources provide you with sufficient guarantees that they meet the requirements or GDPR?

What you need to do

- Check whether any of your users are accessing any non-approved external service which could pose a risk of employees', customers' or any other third party's personal data being shared externally.
- If they are, this service should be blocked immediately.
- Make sure your users/employees understand the importance of never using external resources or cloud-based services other than those approved by the business.

[1] https://www.enforcementtracker.com

[2] https://www.kaspersky.co.uk/small-to-medium-business-security/cloud

[3] https://gdpr-text.com/read/article-28

Kaspersky Endpoint Security Cloud

How we help

Cloud Discovery, a component of Kaspersky Endpoint Security Cloud, lets you discover and then restrict the use of inappropriate or unauthorized cloud resources in your business. Sources of a potential data breach are tracked down and eliminated, helping you maintain compliancy.

GDPR Article 30 'Records of processing activities'[4]

Article 30 requires you to maintain records of processing activities — a labor-intensive requirement that nevertheless brings many advantages. By keeping a register of data processing activities, you can approach your data in a more systematic way, in terms of why data is being processed, storage periods, and third parties to whom data is transferred. In addition, the registry makes it easier to interact with regulators, if necessary.

To do this, you may first need to undertake an inventory and analysis of the data you process. Knowing what data you process and why, and keeping full records of your data processing activities, will also help you identify any gaps in your GDPR compliance overall — see Article 32 below.

What you need to do

- Make sure you know exactly what data you're processing and storing in the cloud services such as Microsoft 365 apps for business, including OneDrive, SharePoint Online and Teams.
- Make sure your reporting shows where data is being stored, and how.
- Find out whether any files containing personal data are being shared outside the business, and where.
- If they are, take any remedial action that might be needed (this could be something as simple as having a word with the file's owner).

How we help

Data Discovery, a component of Kaspersky Endpoint Security Cloud:

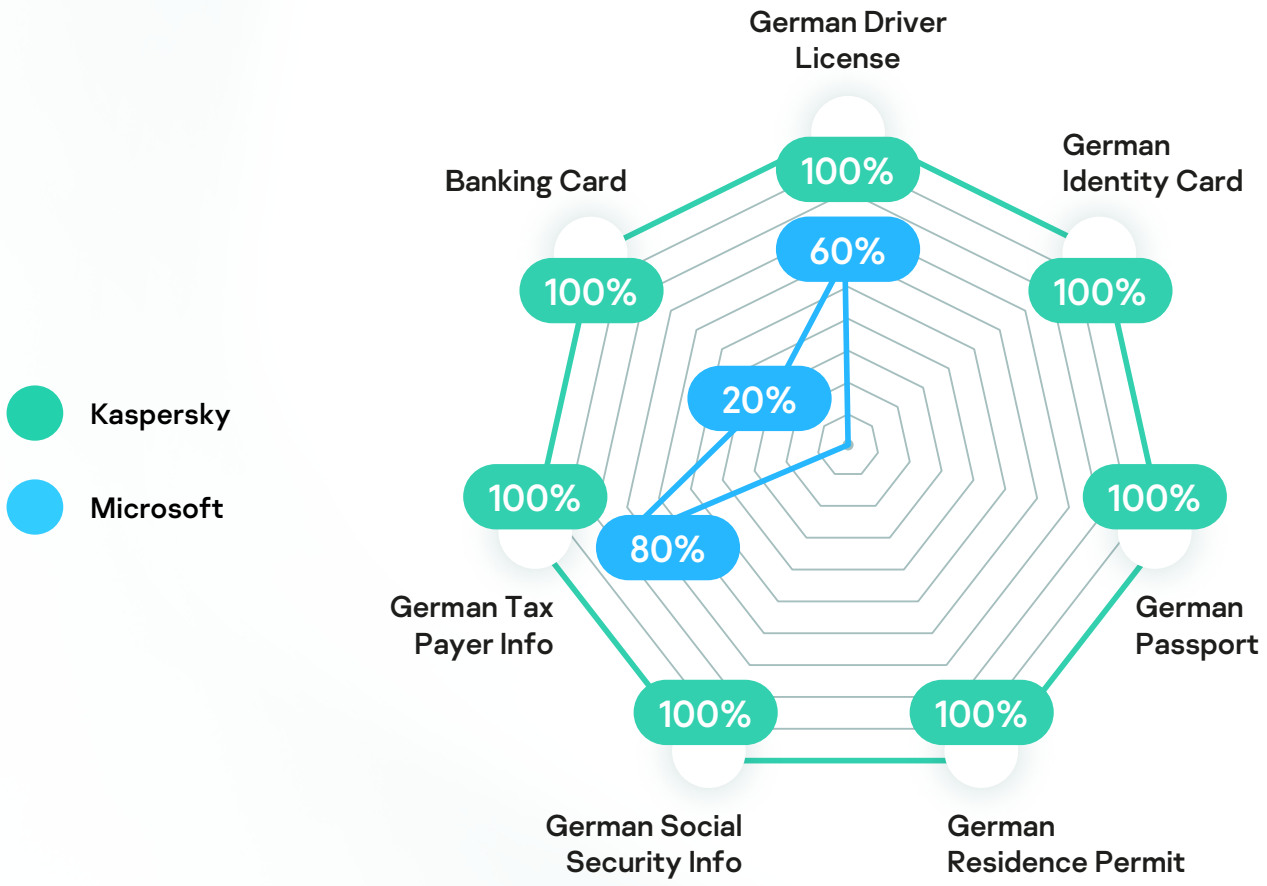
- Helps to control the processing and storing of data in Microsoft 365.
- Discovers and provides visibility into the location, and context of all your data in the cloud.
- Detects personal data in both structured and unstructured data formats.

[4] https://gdpr-text.com/read/article-30

Can you rely on Microsoft 365 DLP capabilities?

You can, but we also recommend that you give some thought to the data discovery performance of the 3rd party solutions. Independent test authority AV-TEST[5] recently performed the same Sensitive Data Discovery Test on Kaspersky Endpoint Security Cloud and on MS Office 365 E5™, using a series of German personal data test cases[6].

The results speak for themselves. Kaspersky achieved a discovery rate of 100% with no false positives. MS Office 365 performed very differently — see below:



Should I buy a separate DLP solution to help with remediation?

Interestingly, our own beta testing[7] has shown that the average SMB organization only holds around 160 files with sensitive data in their cloud storages, with only 15% of these, or about 24 files, being shared outside the business.

So while these checks are extremely important, remediation on this scale doesn't actually take up much time. In view of this, we wouldn't recommend investing in expensive specialized DLP solutions at this level.

Continuous reporting from Kaspersky Endpoint Security Cloud and the occasional manual fix of a risky share are enough to keep you compliant here.

[5] https://www.av-test.org/en/about-the-institute

[6] AVTEST. Personal Identifiable Information Protection: Sensitive Data Discovery test

[7] According to anonymized statistics of events detected by Kaspersky Endpoint Security Cloud during beta testing. The statistics consist of depersonalized metadata voluntarily provided by Kaspersky customers

GDPR Article 32 'Security of processing'[8]

Article 32 requires you to ensure a level of data security appropriate for the level of risk presented by processing personal data, and to ensure that anyone with access to personal data doesn't process that data except under your instructions and in accordance with the requirements of the laws.

This, then, is the big one. There's a degree of flexibility as to how you do this, though you do need to document your evaluation of the measures you take, demonstrating that you've accurately assessed your data processing and risk profiles, appraised the latest tools available and drawn up the associated costings.

What you need to do

- Assess your levels of data security risk — measure the consequences of potential data security breaches for subjects.
- Look at where you're storing data — see Articles 28 and 30 above.
- Look at why you're storing data, and for how long.
- Find ways to control user access to data — and particularly the ability to export data out of the business.
- Implement data protection mechanisms such as encryption on mobile devices.

How we help

- **With breach identification**
  The Data Discovery component of Kaspersky Endpoint Security Cloud helps detect the processing and storing of personal data in services that can be accessed by external parties, which could lead to a potential data breach.
- **With data retention**
  Data Discovery also helps you discover data that's been stored longer than necessary, or longer than specified by your data retention policy.
- **With preventing the export of sensitive data**
  The Device control component of Kaspersky Endpoint Security Cloud prevents users from connecting external and removable devices (other than those approved by the IT department) to their computers in order to physically export (or import) data.
- **With data protection on lost or stolen devices**
  Remote full disk encryption of via BitLocker through the Encryption management component of Kaspersky Endpoint Security Cloud keeps all personal and corporate data protected if a device is lost or stolen.

[8] https://gdpr-text.com/read/article-32

Fines for non-compliance

For especially severe GDPR compliance violations, the fine framework can be up to 20 million euros or 4% of the total worldwide annual turnover. But even the catalogue of fines for less severe violations goes up to 10 million euros or 2% of the turnover.

In Short

GDPR Compliance is non-negotiable, no matter what the size or type of your operation — data leakage doesn't just lead to being fined: it can be a serious blow to your organization's reputation, damaging your customers' trust in you.

But compliance doesn't need to be an onerous process. Most of the requirements laid out in GDPR articles are things you're probably doing already, or should be doing. It's just a matter of formalizing things — making sure you have full ongoing visibility of all the data you store and process, and that you're generating accurate reporting.

The right security software can help a great deal here, without involving you in extra work or heavy costs.

Try now

Kaspersky Endpoint Security Cloud

Learn more

Stay compliant with minimal hassle

GDPR

www.kaspersky.com