



ManageEngine

Guide to overcoming
BREXIT'S
Data management challenges.

Understand Brexit and the data law
modifications it may cause

Contents

- What is Brexit?
- Understanding the withdrawal agreement and no-deal Brexit
- How will Brexit affect Businesses and Trade
- Brexit's effects on data management and IT departments
- How will Brexit affect the GDPR
- Why should data management be the priority for businesses during Brexit
- GDPR-compliant businesses will sail past Brexit easily
- How can ManageEngine help businesses with Brexit



Businesses around the globe are already struggling to become compliant with new data protection laws like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Lei Geral de Proteção de Dados (LGPD). Adding to those challenges, here comes a political and economic change for Europe and the United Kingdom: Brexit.

Brexit is set to happen on January 31, 2020, and will bring a lot of changes to the way businesses operate in the UK and Europe. Any business that has customers, suppliers, or distributors in the UK and Europe will be affected by this change in the European Union. In this e-book, we'll discuss Brexit's impact on IT management and security, and how businesses can resolve these challenges post-Brexit.



What is Brexit?

On June 23, 2016, the UK electorate under Prime Minister David Cameron's administration conducted a referendum to decide whether the UK should remain part of the EU. The result of the referendum was the decision to leave the EU. Brexit is the process by which the UK leaves the trade, economic, political, and operational commitments with other European countries.

When the UK was part of the EU, it enjoyed a single trading area with other EU nations, with no border checks or tariffs; however, post-Brexit, the UK and EU will operate separately. All decisions over immigration and the import and export of goods, services, and capital between the UK and the EU will be defined during Brexit.

All of these changes from Brexit mean that businesses with ties to UK or EU citizens' personal data may need to modify their business model substantially; if the transition post-Brexit is not properly orchestrated, it could affect businesses significantly.

Understanding the withdrawal agreement and no-deal Brexit

Brexit could happen one of two ways: with a withdrawal agreement or no-deal Brexit. A withdrawal agreement would give organizations some breathing room to make the transition post-Brexit. If a withdrawal agreement is reached, the transition period would [likely end on December 31, 2020.](#)

In the event of no-deal Brexit, the UK will leave the EU abruptly without any transition period. No-deal Brexit could have tremendous effects on businesses both inside and outside of the UK.

How will Brexit affect businesses and trade?

Brexit will affect most verticals, except for niche spaces like farming and medical research. According to the [Operation Yellowhammer document](#) released by the EU, large businesses will be able to handle the transition post-Brexit, but SMBs are likely to suffer from this political move. Businesses of any size will not be able to enjoy the benefits of free trade with the EU, and should be redefining their business procedures, and perhaps their corporate-level strategies, to adapt and ride out the outcomes of Brexit.

Here are the major areas where businesses will be affected by Brexit:

- Import and export of goods and services with EU countries, including **VA payments and customs duties.**
- Employment changes for EU citizens in the UK, and vice versa, from restrictions on immigration between the EU and the UK.
- Public transportation, logistics, trademarks, patents, and copyright. Ports could be highly crowded, and business travel will be modified.
- Packaging and labeling changes to move from EU references to UK ones.
- Data collection, storage, processing, and deletion.
- Relationships with partners, suppliers, and distributors, as well as existing mergers. Companies should have a backup plan to forge new alliances post-Brexit.

Brexit's effects on data management and IT departments

Of the areas mentioned above, IT departments will be the most concerned with how Brexit modifies the data management requirements their organizations need to follow. UK organizations are currently required to comply with the EU's GDPR, but that is likely to change once the UK has officially left the EU.

How will Brexit affect the GDPR?

Brexit could have three different effects on the data regulations UK businesses have to follow:

Case 1: UK businesses will continue to be required to comply with the GDPR until the UK can come up with its own personalized data protection regulation.

Case 2: The UK will go back to its Data Protection Act 1998 (DPA). Considering the DPA is not well-defined or written to handle the latest technological developments pertaining to personal data, this is unlikely to happen.

Case 3: The UK will define new data protection norms that fall somewhere between the DPA and the GDPR until it can roll out a new regulation.

If the UK decides to go with the last two options, the EU will not define the UK as a “secure third country,” a country that has shown proof of adequate data handling for securing EU citizens’ personal data. If the UK is not defined as a secure third country, businesses cannot import personal data from EU databases into the UK.

Businesses in the UK should be prepared to move any data that is being stored in the EU back to the UK, and vice versa. Personal data collected by UK organizations from EU citizens also needs to be revisited as per the outcomes of Brexit. Either UK organizations will be asked to get reconfirmation from EU data subjects, or they’ll be forced to remove EU data subjects’ personal data.

Data centers handling cross-country personal data need to be verified, scrutinized, repositioned, and managed as per Brexit guidelines that are declared either at the end of January 2020 or after the transition period.

Why should data management be a priority for businesses during Brexit?

With so much uncertainty surrounding the outcome of Brexit, many businesses are concerned about what the future holds; some companies have already seen their normal operations be complicated by Brexit.

Above all that, the UK's economy has [become stagnant](#) due to the delayed decision on Brexit. The food and beverage industry has started to see inflation, and it is [believed that the same trend](#) could spread to other verticals as well.

Brexit may affect industries differently, but it will cause significant changes to one thing all organizations have: data. Whether it's customer data, supplier information, business deals, or some other form of business data, Brexit will likely change the way businesses manage it. Organizations will need to respond to the new data regulations that are likely to follow Brexit, which means organizations may need to modify their data management strategy and sustain the new practices until they have mastered them.

Achieving all of this in a short span of time without proper planning could be difficult, which is why businesses need to equip the right data management practices now to sail past the uncertainty around Brexit.



GDPR-compliant businesses will sail past Brexit easily

Businesses that are already compliant with the GDPR will have a smooth transition during Brexit. The GDPR is the most comprehensive data protection law in the market right now, and the UK is most likely to retain the GDPR instead of implementing its own data regulation. If the UK decides to retain the GDPR, the EU and the UK will need to come to an agreement to develop adequate safety measures in the UK, consider the UK a secure third country, and then finally import data from EU countries.

Businesses that have the following data management and security strategies will easily meet any new data management challenges that arise from Brexit:

- Collect only the relevant data.
- Process data as per their privacy policy.
- Share data with third parties as mentioned in their policies.
- Store data in the locations mentioned in their privacy policy.
- Allow data subjects to access and modify their personal data.
- Delete data within the time frame mentioned in their privacy policy.

However, businesses that are still working on complying with the GDPR, or not at all concerned about the GDPR until now, need to start building a substantial amount of data management policies to get past Brexit.

While the GDPR focuses on organizations that deal with a substantial amount of data, the new regulations that may follow Brexit could force stricter data management requirements on individual entities in the UK and the EU, like small organizations or freelancers. Many businesses in the UK and the EU will be obliged to comply with both the GDPR and whatever data regulation follows Brexit, and they'll only have until the end of the transition period (if it is a withdrawal agreement) or by January 31, 2020 (assuming no-deal Brexit).



How can ManageEngine help businesses with Brexit?

In terms of adapting to Brexit, ManageEngine can assist businesses from a data management and information technology perspective. ManageEngine has already assisted organizations around the EU in becoming GDPR-compliant using its suite of IT management tools, including Desktop Central, Mobile Device Manager Plus, Device Control Plus, Password Manager Pro, and Data Security Plus. These same tools can be used to effectively manage IT security and data in the case of Brexit too.

ManageEngine
Desktop Central

Desktop Central for unified endpoint management

ManageEngine's unified endpoint management software Desktop Central helps businesses manage their servers, desktops, laptops, and browsers from one central location. It also helps in organizing corporate data with its standalone [Data Protection Officer \(DPO\) dashboard](#). This dashboard offers a complete overview of inbound and outbound data, existing data, idle data, and more, helping businesses harden their data security and gain control over their corporate data spread across countries.

Desktop Central's DPO dashboard can help businesses:

- Restrict data transfers through USB drives.
- Prevent data breaches through stale or inactive user accounts.
- Define the right firewall and wireless configurations.
- Define strong passwords.
- Monitor incoming and outgoing data.
- Identify and remove any unwanted mapped network drives and networkshares.
- Remove elevated privileges from users that don't need them.
- Restrict browser-based data access.
- Patch critical vulnerabilities on time to avoid zero-day attacks, including remote code execution, privilege escalation, and other patch based cyberthreats.

Businesses that already own Desktop Central can make use of the DPO dashboard right away. For organizations that are yet to download Desktop Central, it's high time they consider doing it.

With the right data management strategies in place, businesses can easily sail past Brexit. Download Desktop Central now to make this political transition much smoother for IT departments.



[Get a personalized demo](#)

[Request a quote](#)



ManageEngine Device Control Plus

Device Control Plus for data leakage prevention

While Desktop Central can help organizations manage their endpoints, Device Control Plus offers more tight controls over data transfer and devices. Device Control Plus can help businesses prevent data leaks using its:

Desktop Central's DPO dashboard can help businesses:

- File access and transfer control.
- Port and device access management.
- Ability to grant temporary access to devices.
- Zero Trust approach towards devices.



[Get a personalized demo](#)

[Request a quote](#)



Mobile Device Manager Plus

Mobile Device Manager Plus for mobile device management

With enterprise mobility management capabilities, Mobile Device Manager Plus can assist businesses in securing their corporate data stored on mobile devices. A few of its key capabilities include:

Desktop Central's DPO dashboard can help businesses:

- Remote wipe
- Mobile content management (MCM)
- Mobile application management (MAM)
- Containerization
- Email security management
- Geo-fencing
- GPS tracking

TRY MOBILE DEVICE
MANAGER PLUS

[Get a personalized demo](#)

[Request a quote](#)

For more information about
Password Manager Pro and **Data Security Plus**,
visit www.manageengine.com

About the author



Giridhara Raam



Giridhara Raam is a cybersecurity evangelist, data protection laws researcher, author, speaker, blogger, and product marketer at ManageEngine. His passion for cybersecurity is rivaled only by his love for football and FC Barcelona.

ManageEngine 

