



LINK11

**“KEEPING YOU SECURE,
KEEPING YOUR DATA
IN EUROPE”**

KEN MACINTYRE
Sales Director UK & Ireland

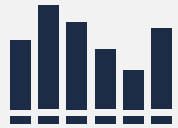


**Politically
motivated attacks
on critical sectors
in Europe are
increasing**

Killnet, NoName057(16) and Anonymous Sudan are on the rampage.

- May 2022, cybersecurity agencies from the US, Australia, Canada, New Zealand, and the [United Kingdom](#) released a joint Cybersecurity Advisory.
- [Public sector digital infrastructure](#) is a prime target for cyberattacks during times of political unrest and economic instability.
- DDoS attacks are used to [exert political pressure, sabotage critical infrastructure, or hold it for ransom.](#)

UK PARTICULARLY AFFECTED



14%

increase in the number of cyberattacks experienced by UK councils



39%

of UK businesses detected cyberattacks



43%

of the cyberattacks reported in Europe are in UK

The energy and financial services sectors in the UK were the most affected, accounting for **32% of all attacks.**

RECENT NEWS

SC MEDIA
A CyberRisk Alliance Resource

TOPICS EVENTS PODCASTS RESEARCH RECOGNITION LEADERSHIP

Identity and access, Threat intelligence, Network security

f t e in

Killnet DDoS attacks against healthcare dip as identity risks tick up

[Jessica Davis](#) April 7, 2023

DIGITAL JOURNAL WORLD TECH & SCIENCE SOCIAL MEDIA BUSINESS ENTERTAINMENT LIFE SPORTS Q

BUSINESS

Capita cyberattack proves all businesses remain vulnerable

By [Dr. Tim Sandle](#) Published April 5, 2023

PRIVACY Affairs News Research Security Guides Experts About Q SEARCH

Home » News » UK DDoS

Russian Hackers Target UK Government Institutions with New DDoS Attacks

By [Miklos Zoltan](#) 31 March 2023
Founder - Privacy Affairs

The Russian hacker group NoName has targeted today several UK institutions and organizations. The DDoS attacks resulted in the affected websites becoming temporarily unavailable.


Our Mission
We believe security online security matters and its our mission to make it a safer place.

POLITICO Enter keyword Q EXPLORE NEWSLETTERS & PODCASTS POLITICO PRO

FROM POLITICO PRO

European Parliament website hit by cyberattack after Russian terrorism vote

One official blamed pro-Russian hacking group Killnet for the DDoS attack.



"I confirm that the Parliament has been subject to an external cyber attack" said Dita Charanzová | Ludovic Marin/AFP via Getty images

BY SHANNON VAN SANT AND CLOTHILDE GOUJARD
NOVEMBER 23, 2022 | 4:46 PM CET | 2 MINUTES READ



PREVENTION
HIGHLIGHTS
GAP IN GDPR
COMPLIANCE

GDPR AND ITS CONSEQUENCES – WHAT TO LOOK OUT FOR WHEN CHOOSING A CDN PROVIDER AND DDOS PROTECTION

With the implementation of the [General Data Protection Regulation \(GDPR\)](#) in 2018, companies operating in the EU must prioritize protecting their customers' personal data.

[CDN and web DDoS protection](#) providers headquartered outside the EU and UK cannot guarantee that data will be processed in a GDPR-compliant manner.



GDPR AND ITS CONSEQUENCES

In 2020, The Schrems II judgement, handed down by the European Court of Justice, has further complicated the issue.

The judgement invalidated the Privacy Shield framework, which previously allowed companies to transfer personal data from the EU to the United States

Companies working with non-European CDN and web DDoS protection providers face harsh penalties if they violate the General Data Protection Regulation.

To avoid any risks, working with European providers is the best idea.



Have you or your clients had to complete a Transfer Risk Assessment?



Transfer risk assessments

Share



Download options



Search this document



[About the Guide to the GDPR](#)

[What's new](#)

[Key definitions](#)

[What is personal data?](#)

[Controllers and processors](#)

[Principles](#)

[Lawfulness, fairness and transparency](#)

[Purpose limitation](#)

In brief

UK GDPR contains rules about transfers of personal data to receivers located outside the UK, which we refer to as restricted transfers.

One way to comply with UK GDPR rules on restricted transfers is to put in place an Article 46 transfer mechanism. These are the "appropriate safeguards" listed in Article 46 of the UK GDPR. Examples are the ICO's International Data Transfer Agreement (IDTA), the Addendum to the EU SCCs (the Addendum) and Binding Corporate Rules (BCRs).

If you are relying on an Article 46 transfer mechanism you must carry out a transfer risk assessment. This risk assessment will help you consider whether, in the circumstances of the transfer and with your chosen Article 46 transfer mechanism in place, the relevant protections for people under the UK data protection regime will be undermined.

Why choose a European provider?



Reliable and cost-sensitive

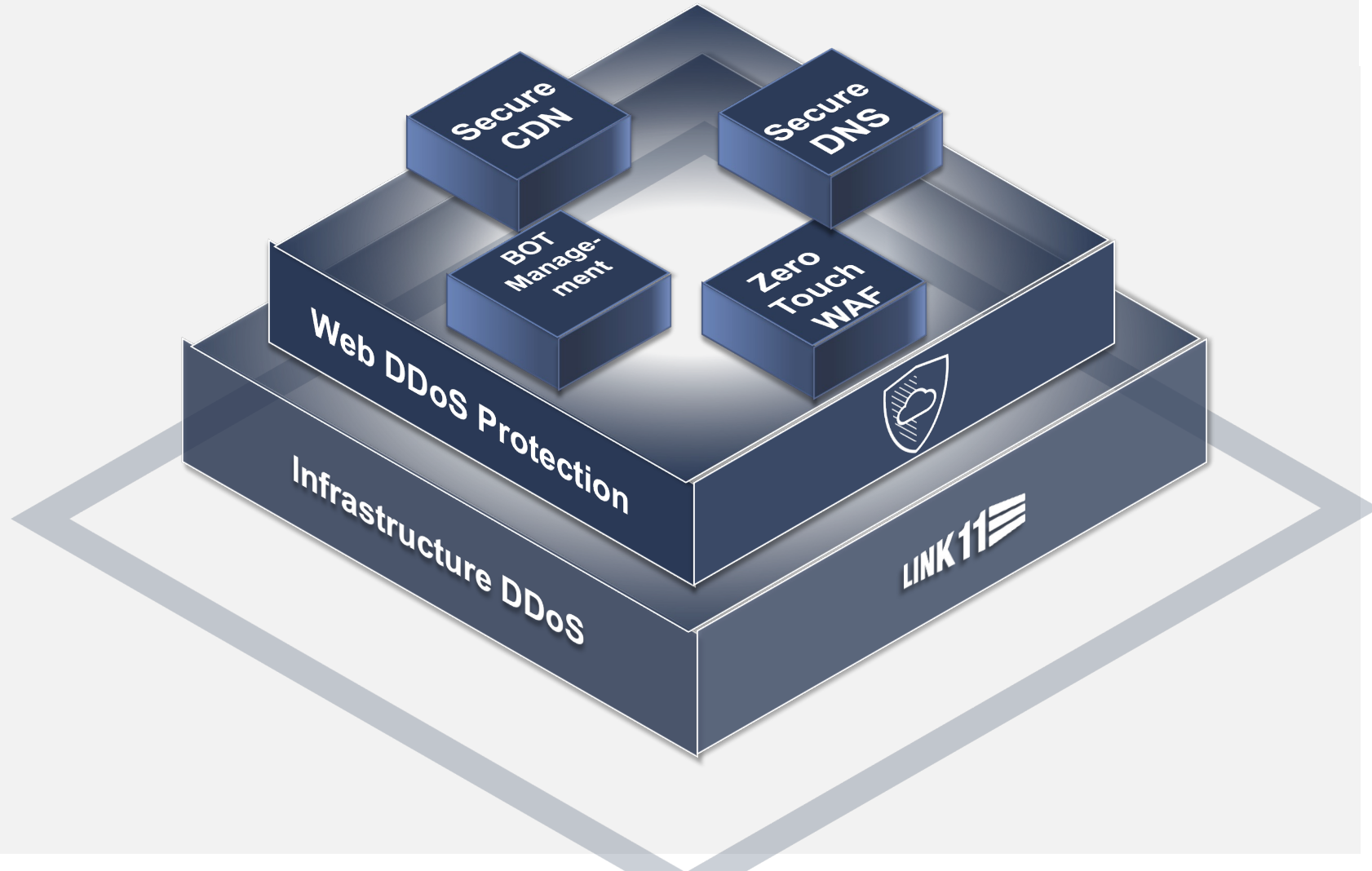
The costs for compliance with European data protection regulations quickly add up due to corresponding contract add-ons.

Risk assessment and impact assessment – companies have a responsibility

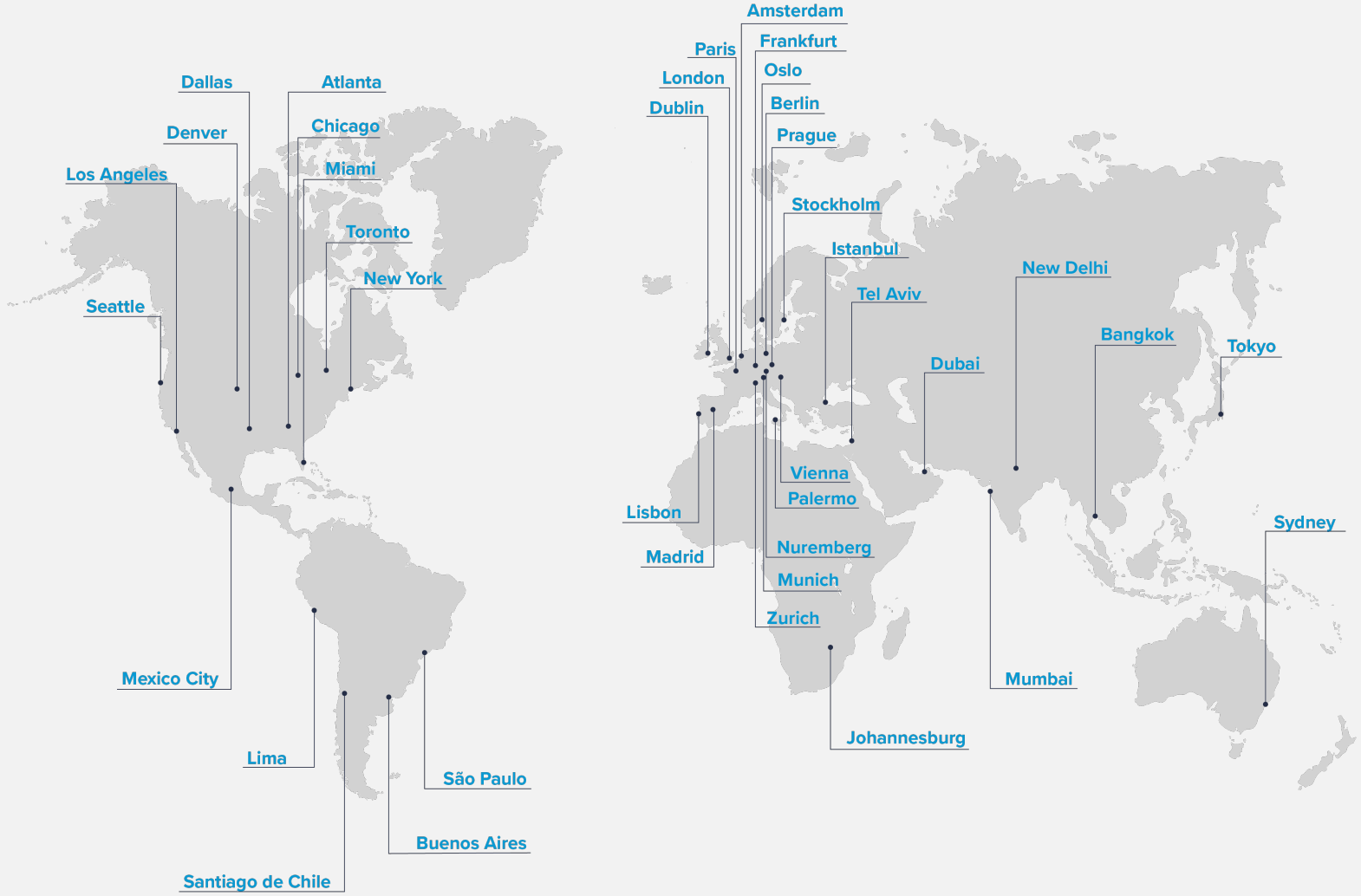
Companies must conduct a Transfer Impact Assessment (TIA) or Transfer Risk Assessment (TRA) for each vendor they work with. These assessments are costly and complex

Keeping your Data Secure Keeping your Data in Europe

Link11, as a provider
headquartered in
Europe, fulfils all
requirements.



OUR GLOBAL NETWORK





QUESTIONS
AND
ANSWERS



KEN MACINTYRE
Sales Director UK & Ireland

k.macintyre@link11.com
+44 7408 817631



CONTACT