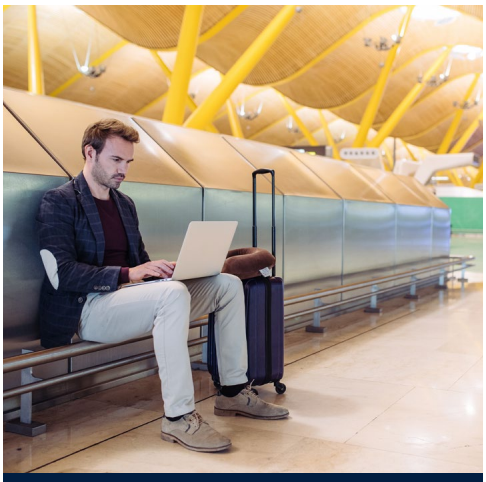
ABSOLUTE FOR GDPR COMPLIANCE

STAY COMPLIANT WITH PERSISTENT ENDPOINT VISIBILITY AND CONTROL



THE CHALLENGE

Whatever the means, the result is the same: if you've received a deletion request and can't be sure of all the places that data is stored, you're at risk. All it takes is one unseen endpoint to incur a breach and financial penalties — not to mention lost consumer trust.

DATA RIGHTS ARE HERE TO STAY

The EU's Global Data Protection Regulation (GDPR) was a wake-up call when it was introduced in 2018. With 72-hour requirement for reporting breaches, and clear-cut data rights for EU citizens, GDPR provides for hefty penalties for violations — so any company that deals with EU citizens should take significant steps to prevent breaches and protect data.

Hundreds of organizations large and small have already received fines, ranging from €90 to €50,000,000. Although GDPR enforcement is ramping up, misinformation and ignorance abound. This solution sheet highlights key areas of focus and illustrates how Absolute can help you attain and maintain GDPR compliance at all levels of your organization.

PERSONAL DATA IS THE CORNERSTONE OF GDPR

Breaches make headlines, but lax data protections make breaches possible. **The core change brought about by GDPR the establishment of rights regarding EU citizens' personal data.**

"Personal data" has a very broad definition. It's not just driver's license numbers or financial information — it's any information that pertains to an identified person, or a person who could indirectly be identified by your data.

If you collect or use that information, you have a responsibility to:

- Delete or change it if requested (the "Right to Be Forgotten")
- Transfer or release it to the users it pertains to (the "Right to Data Portability")
- Do these at the user's request, "without undue delay" (generally less than 30 days)

To many IT and security professionals, these may seem like simple requests. But in reality, things are complicated. Staff may download spreadsheets containing that data onto their hard drives. You might not find it because the device doesn't call into the network regularly. Or maybe certain endpoint management agents aren't working on that device.

Whatever the means, the result is the same: **if you've received a deletion request and can't be sure of all the places that data is stored, you're at risk.** All it takes is one unseen endpoint to incur a breach and financial penalties — not to mention lost consumer trust. You still need to defend against breaches and attacks, but your efforts are in vain if you don't have visibility.

ABSOLUTE GIVES YOU THE TOOLS AND INTELLIGENCE TO SECURE PERSONAL DATA

You need to be able to continuously monitor all of your devices — and to delete or secure data as soon as issues arise. Enter Absolute, the only resilient endpoint security solution that is factory-embedded in the firmware by every major PC

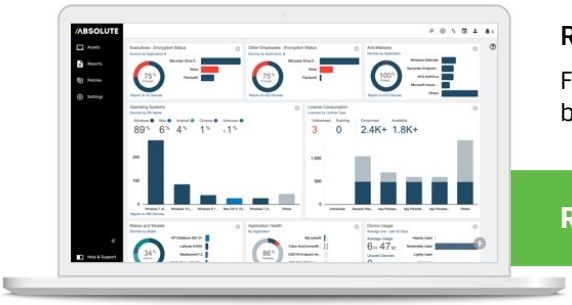
manufacturer. **So, even if a device is off your network or the user has disabled your controls, Absolute reasserts your visibility and control as soon as it connects to a network.** Any network.

In the scenario we just discussed, you'd be able to remotely activate Absolute on all compatible devices, giving you complete visibility into their location and the health of your security apps. Discover tools instantly highlight all instances of personal data, giving you the power to remotely remove or secure it.

And setup is easier than you'd think — with over 500 million devices already shipped with Absolute embedded, chances are, all you have to do is activate it.

SEE HOW WE CAN HELP YOU

Forge a path towards better data security with a self-healing security solution for all your endpoints, apps, and data. Set up a live demo to see how Absolute can help your organization.



REQUEST A DEMO

Find out how our solutions can benefit your organization.

REQUEST DEMO

ABOUT ABSOLUTE

We help organizations recover and resume normal operations in the face of security breaches.

Absolute envisions a world where security and IT professionals always retain control over their devices and data. We're the first and only company to offer uncompromised visibility and near real-time remediation of security breaches at the source.

Absolute Persistence™ returns devices to their desired state of safety and efficacy after malicious attacks or user error, thanks to our unique location in the firmware of more than 500 million devices built by most of the world's top device manufacturers.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com

Absolute's tools for securing GDPR data

ENDPOINT DATA DISCOVERY
Determine if any of your sensitive data is on at-risk devices

REMOTELY DELETE DATA
Remove some or all of the data from a compromised machine

ALERTS AND WIDGETS
Get notified as soon as your essential security apps are damaged or disabled

APPLICATION PERSISTENCE
Ensure your security apps, like encryption or VPN, are able to heal themselves

GEOFENCING
Detect unauthorized movement of any device you choose

REMOTE DEVICE FREEZE
Lock down a compromised machine until a user returns it or you take remedial action

GDPR compliance can seem daunting, but with complete visibility and control of your endpoints, you can identify and protect EU personal data — no matter where it's hiding.

Learn more about how Absolute addresses GDPR requirements, with the ability to monitor and secure PII, prevent data breaches, and automate remediation now at absolute.com/gdpr