Datasheet

Data Privacy with PowerDMARC

One of the biggest concerns organizations face when implementing DMARC is how securely we handle their data. You might be wondering how much visibility our monitoring systems have on your data.

Here's the thing—PowerDMARC's servers **do not host any private information** belonging to our clients. The only data we receive are your DMARC reports and the DMARC alignments of your emails.

But how much personal information do DMARC reports contain? How securely are they stored?

Let's go over every concern people have with DMARC and show you how PowerDMARC keeps your data secure.

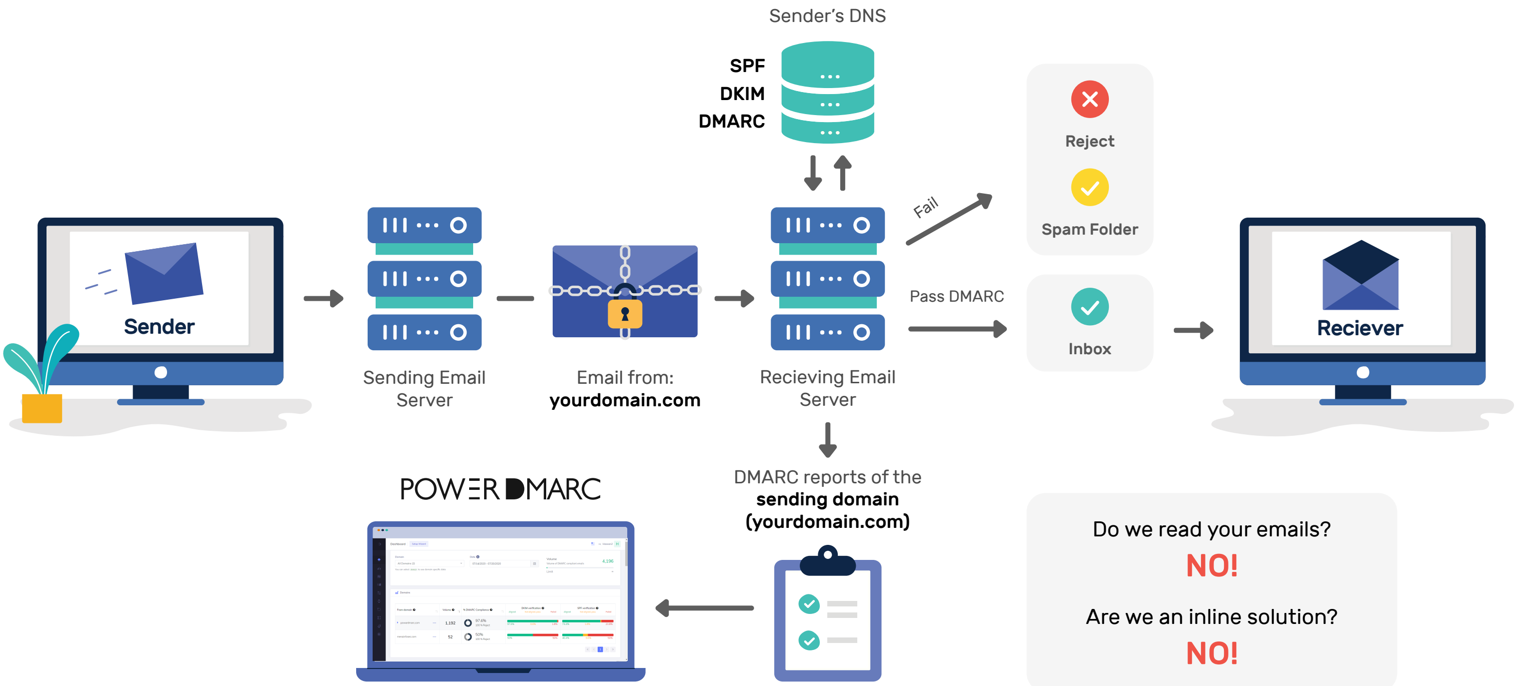
Your Domain

PowerDMARC does not read your emails

Email servers use DMARC to check the authenticity of an email and send reports, which are processed by PowerDMARC. At no point do we have access to your inbound or outbound emails.

Our systems only monitor domain activity

We only monitor the IP addresses sending email from your domain to look for suspicious activity. We don't view the contents of your emails.



Do we read your emails?

NO!

Are we an inline solution?

NO!

DMARC Aggregate Reports

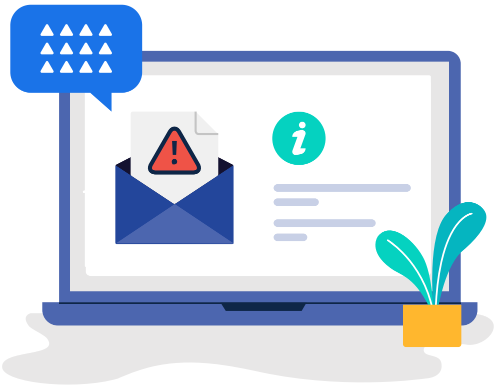
DMARC Aggregate reports **do not contain** any private or personally identifiable information (PII). They just provide a daily overview of:

- The email receiver that sent the report
- Number of emails sent from your domain
- Emails that passed/failed DMARC, SPF and DKIM
- IP addresses that sent email from your domain

DMARC Forensic Reports

DMARC Forensic reports are only sent when someone is potentially trying to spoof your domain, or your email fails DMARC, SPF or DKIM for some reason.These **may potentially contain** private or sensitive information, although email receivers typically don't send any private information in Forensic reports anymore. They generally include:

- Your 'From' domain
- Time email was received
- IP address of servers that sent emails from your domain
- Subject line
- DMARC, SPF and DKIM pass/fail results
- Headers of the failing email



But we can make it even more secure!

PowerDMARC gives you the option to encrypt your Forensic reports. To make this absolutely secure, you can use your own PGP key pair to encrypt the reports.

PowerDMARC Platform compliance:

PowerDMARC is ISO 27001/PCI-DSS/GDPR/California Consumer Privacy Act (CCPA) compliant.

PowerDMARC is all about low-profile, high security email protection.

Our services are designed to make it easy and intuitive to maintain a high level of security in your domain. Your private information belongs to no one but you, and PowerDMARC makes sure of that.