

February 22, 2018

Spambrella® - Spambrella & The GDPR

HOW SPAMBRELLA CAN ASSIST CUSTOMER COMPLY WITH THE EU GDPR



EMEA – UNITED KINGDOM HQ

Spambrella Ltd - 70 Churchill Square Kings Hill,
West Malling, Kent, ME19 4YU, United Kingdom

USA, CANADA – NEW YORK HQ

Spambrella LLC, 295 Madison Avenue, 12th Floor, New
York City, NY 10017, United States - Tel: 917 410 8066

www.spambrella.com - Copyright © 2018 Spambrella | All rights reserved

Spambrella is not in the business of providing legal counsel and this document is not intended to provide, and should not be construed as, legal advice.



INTRODUCTION

On 25 May 2018, the most extensive and far-reaching piece of European data protection legislation will come into force—the European Union’s (EU’s) General Data Protection Regulation (GDPR) will replace the 1995 European Union Data Protection Directive.

At its core, the GDPR aims to put EU residents in control of their personal and sensitive data. It regulates how their data is collected, processed, stored, deleted, transferred, and used. Any company that does business in the EU or handles the personal data of EU residents is obligated to comply with the regulation.

This applies to all companies processing personal data of EU residents—even companies that do not have physical operations in the EU. For any company collecting personal data on people located in the EU or for any company doing business in the EU, GDPR compliance is mandatory. Regardless of where data is processed, the GDPR requires that personal information be protected.

Developing a plan to comply with the new rules is critical for all organizations, including Spambrella. Spambrella is committed to compliance with the GDPR across our solutions and services. As a data processor, we maintain the privacy and confidentiality of the personal data entrusted to us.

This document details how Spambrella cloud-based solutions comply with the seven key principles of the EU GDPR.

GDPR MANDATES NEW CONTROLS



www.spambrella.com - Copyright © 2018 Spambrella | All rights reserved

Spambrella is not in the business of providing legal counsel and this document is not intended to provide, and should not be construed as, legal advice.



SPAMBRELLA

Spambrella helps organizations secure and control inbound and outbound email. It stops malware and non-malware threats such as phishing, impostor email, and business email compromise (BEC) attacks. It provides granular filtering to control bulk "graymail" and other unwanted email. And business continuity capabilities keep email communications flowing, even when email servers fail. Spambrella provides the tools organizations need to keep their employees safe from email threats.

To deliver services, Spambrella processes personal data embedded in emails. Personal data processed includes:

- Names
- Email addresses
- Passwords
- IP addresses
- Location data
- **NOTE:** *Personal data may also be included in email subject lines, email body headers, URLs, message IDs, and attachment names*

The purpose of data collection is limited to providing or enhancing the protection capabilities of the solution.

Recital 49 of the GDPR says every data controller has a legitimate interest in “the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services.... This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.” It is Spambrella’s belief that our service achieves the aims of the GDPR to secure and protect individuals’ privacy in their personal data, and both data subjects and our customers are better secured when protected by Spambrella.

DATA TRANSPARENCY

Right to Access: The primary purpose of Spambrella is to protect employees from emerging threats. Authorized users from organizations can access relevant records from an easy to use console.

www.spambrella.com - Copyright © 2018 Spambrella | All rights reserved

Spambrella is not in the business of providing legal counsel and this document is not intended to provide, and should not be construed as, legal advice.



Right to be Forgotten: Authorized users from customer organizations can delete user records from the admin console. As an example, if an employee leaves the customer's organization, authorized administrators can delete the user stores.

Spambrella will make available to the data controller information that may assist the data controller in demonstrating its compliance with the GDPR.

DATA TRANSFERS

Spambrella maintains that our technology partners are in full compliance with [EU-US Privacy Shield](#) and [Swiss-US Privacy Shield](#) frameworks that facilitate transfers of personal data of the US and the EU and between the US and Switzerland.

In addition, Spambrella willingly enters into contract commitments in the form of data processing agreements (aka Model Clauses or EU Standard Contractual Clauses (SCCs)). Spambrella commits to updating and maintaining new versions of the data processing agreements to include GDPR relevant provisions.

DATA PROCESSING

As the data processor, Spambrella only processes personal data on behalf of the data controller (our customers) and on written authorization from the data controller (i.e. the Spambrella End User License Agreement and Partner Agreement). In addition, we only process data necessary to deliver the Spambrella service. The personal data processed on behalf of the data controller will be accurate, complete, and kept up-to-date as much as technically possible.

Spambrella only stores personal data for the duration of the contract with the data controller, with the following exception: any email caught by Spambrella detected by the service as potentially containing malicious content may be retained (exclusively for the purpose of threat analysis) for up to 15 months (or longer in the case of metadata from message log files), after which time it may be automatically deleted. The length of time data is retained by Spambrella is due to the fact that in order to provide our valuable Email Protection service and protect both the customer's data and data subjects' privacy, it is necessary for some personal data contained within those malicious messages be retained (and in rare cases the entire email that contains malicious content may be retained). All logs and reports are encrypted in transit.

DATA SECURITY & PRIVACY

Spambrella ensures that adequate technical and administrative controls are implemented to protect the integrity and confidentiality of personal data against accidental or unauthorized loss, alteration, destruction, or access.

Access controls mechanisms are established and all the physical and logical accesses are logged and analyzed. Spambrella only allows access to personal data by privileged Spambrella personnel.

www.spambrella.com - Copyright © 2018 Spambrella | All rights reserved

Spambrella is not in the business of providing legal counsel and this document is not intended to provide, and should not be construed as, legal advice.



Logical access is performed using two-factor authenticated systems and all the privileged access is restricted to a subset of the operations team.

Physical security controls of the facilities include cameras, vehicle blockades, parking lot design, bulletproof glass/walls, and unmarked buildings. All data centers include 24x7 on-site security, multi-factor authentication (including biometrics) and perimeter security that includes unmarked entrances, person traps and video monitoring of all doors.

To maintain the confidentiality of personal data flowing through Spambrella, customers can enable Email Encryption to set policies that encrypt, quarantine, or block emails containing personal information.

Wherever applicable Spambrella deploys encryption and hashing to protect personal information. Data at Rest may, at the data controller's discretion, be encrypted in the Email Quarantine with AES-256. Data in Transit may be encrypted using a TLS session encrypted with a 2048-bit RSA asymmetric key.

STANDARDS AND CERTIFICATIONS

Our data centers are designed with market-leading security and privacy capabilities. Our North American facilities maintain SSAE 16 audit reports and European data center facilities maintain ISO 27001 certifications. Spambrella adheres to the Availability, Confidentiality and Security Trust Principles described by the SSAE 16 standard. Spambrella has implemented a Continuous Monitoring Program to ensure that security controls remain in place and effective on an ongoing basis.

All Spambrella procedural and technical security controls are clearly documented. Annual audits are conducted by a suitably accredited firm to ensure that the documented procedures are followed.