clearswift

Driving GDPR Compliance: Discover, Secure and Govern

The EU General Data Protection Regulation (GDPR) is raising the privacy bar on personal data to strengthen its citizens' digital rights and simplify protection rules across the region—regardless of where the business is located or data is processed. Organizations of all sizes will be required to manage personal data at a whole new level. Discover where it's stored, detect when it's shared, understand its regulatory context and apply the prescribed security measure.

Complying with GDPR effectively without costly disruptions to your business is key and will require real-time:

Data Visibility	Adaptive Security
Intelligent Policy Enforcement	Governance

Data Visibility

You can't protect want you can't see.

Discover personal data distributed and hidden throughout your business, while monitoring information before it leaves through email, web, social media and cloud apps. Let's not forget removable storage devices and often overlooked processes such as the publishing of documents to the corporate website. Gaining such visibility into your data can initially be used as part of a privacy audit, assessing how great the problem of control might be, or at a later point in time, as part of a Data Protection Impact Assessment. However, it can also be used as part of a 'right to be forgotten' request where discovery of the information held in unstructured files on endpoints and file servers is needed. The action of deletion can then be carried out automatically or manually.

Intelligent Policy Enforcement

Not all data, access and sharing rights are created equal. Intelligent polices need to be applied consistently across all channels and based on GDPR geography, data type (i.e. national security, child protection, healthcare, etc.), purpose conditions and required security treatment.

Intelligent policy enforcement uses both context as well as content in making both inbound and outbound policy decisions. The context is the sender and the recipient (or target upload site) as well as the communication mechanism, for example email, web or endpoint. A single shared policy creates consistency as well as ease of deployment and use. A document might be sent by corporate email and the policy action would be to encrypt the communication. However the same file might be uploaded to a cloud collaboration site, in which case the action could be to redact the sensitive information. Finally, the same user might want to copy it to a USB stick, at which point the system can block it.

Clearswift provides a simple interface to build polices to discover and protect the information which is subject to GDPR. It also includes templates to make the process even easier, these include:

Predefined regular expressions for PII (Personally Identifiable Information) and PCI (Payment Card Industry) including:

- National Insurance and ID numbers
- IP addresses
- Credit card numbers
- Social security numbers
- International Bank Account Number (IBAN)

Editable compliance dictionaries, including:

- Personally Identifiable Information (PII)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Securities and Equities Commission (SEC)
- Sarbanes Oxley (SOX)

Contextual policy rules for social network and cloud collaboration sites, including:

- Inbound threat protection
- Inbound compliance violation protection
- Outbound data leak protection
- Adaptive Security

Adaptive Security

Clearswift's GDPR solution is designed to protect all areas of the enterprise and out into the cloud. Protecting the information storage and egress points, see Figure 1, is critical to protecting personal data from losses or leaks through accidental insider mistakes, the malicious insider or malevolent external attacks. Adaptive security applied in real-time based on specific GDPR policy, whether it calls for automated redaction, encryption, blocking, moving or deleting.

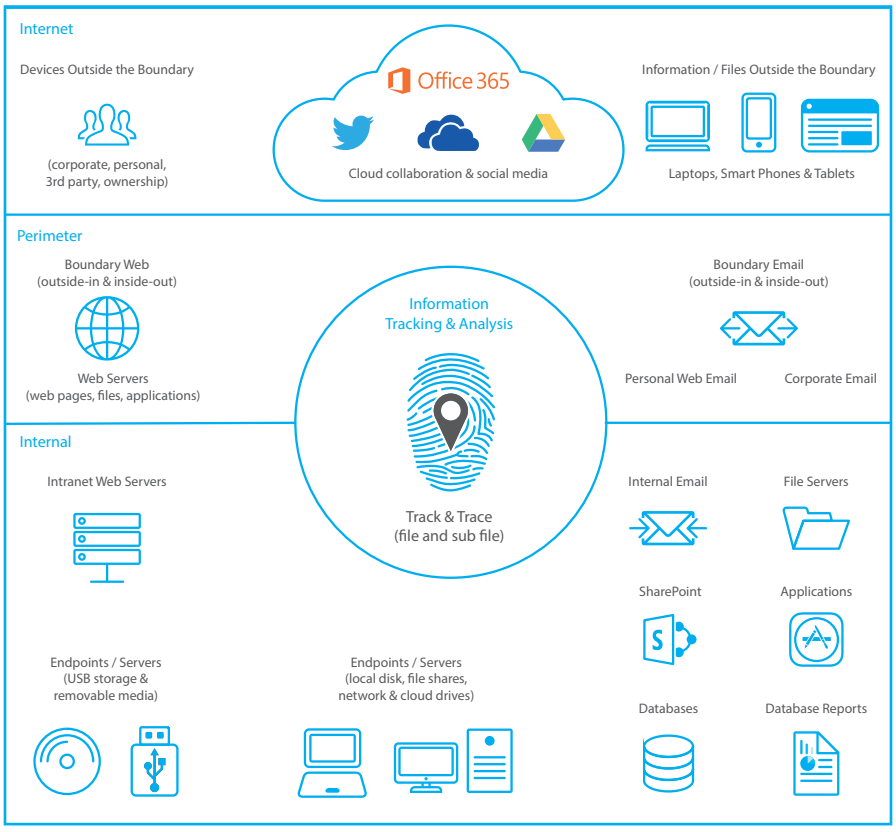

Figure 1: Clearswift solutions provide protection across all areas of the enterprise

Clearswift's unique Adaptive Redaction technology makes GDPR enforcement a reality for most organizations by removing only the required personal data from being shared, allowing the rest of the digital activity to continue without business disruption and false positives. Complete protection that goes unnoticed from the end user, protecting the organization, business partners and the customers.

Governance

Whether you are the Data Protection Officer (DPO), compliance manager or IT security professional, you will need complete visibility into reports, policy violations, quarantined data, logs, etc. Clearswift's GDPR Governance track and trace capability not only enables real-time policy and adaptive security enforcement, but enables violation / breach analysis to identify loss of personal data, sources and exposure required for notifications.

Additionally, the granular tracking of information at a file and a sub-file (information) level helps GDPR to monitor information across the organization boundary to 3rd parties. Information provenance reports can be used to determine which information has been sent to which 3rd party, so the correct organizations can be contacted in the event of a 'right to be forgotten' request being enacted.

Clearswift Solutions for GDPR Compliance

Clearswift has built its business on protecting critical information. Organisations of all sizes rely on its unprecedented level of security to protect information when it is in transit through email, flowing to or from the Internet or while at the endpoint. The key is the Deep Content Inspection Engine which lies at the heart of the solutions. This splits email, Internet traffic and documents into constituent parts in order to carry out analysis. Polices are then applied based on the content and the context of the communication. Including context is important in the decision making process, understanding who is initiating the communication, where it is going and how it is getting there adds to what action or actions need to be carried out in order to comply.

Clearswift's deeper level of inspection and sanitization goes beyond what is traditionally offered in the market, it is not limited by zip/encryption, file size, analysis timing delays, virtual environment evasion techniques or multiple embedded document layers. As a result, it offers amongst the highest detection rates, low impact (i.e. nearly eliminates false positives) and overall offers a more cost-effective approach to comply with GDPR.

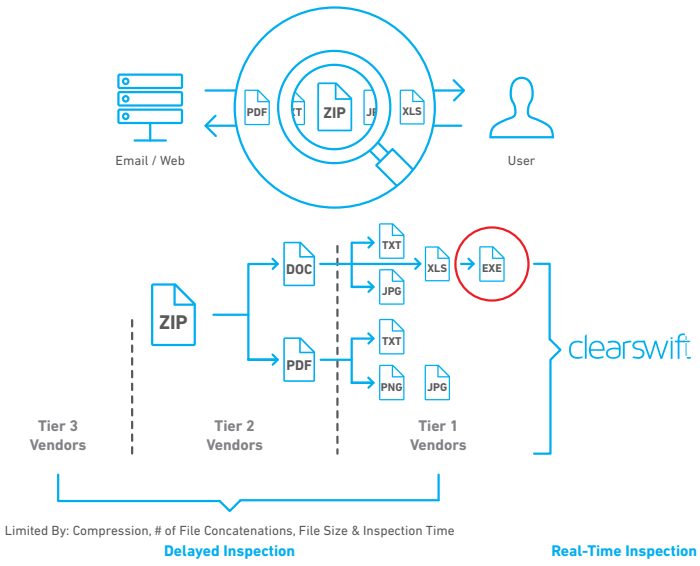

Figure 2: Deep inspection at the most granular level: file/sub-file, encapsulated, hidden & metadata

Peering

Organisations can prepare and phase their GDPR solution roll-out by risk priority, department and/or resource availability without having to deploy all at once. Initial investigations into information flowing across corporate email can be augmented with an added layer of inspection and sanitization at the web/cloud to look for that same information across all exit points. Peering ensures that the policy is shared across the channels and any changes are quickly and consistently replicated across the communication flows. Administration is carried out from a single console with new options appearing as different solution components are added.

Flexible Deployment Options

Clearswift's GDPR solution can be activated on existing Clearswift Gateways (+Critical Information Protection for endpoints) or enhances the investments already made in existing IT security tools (i.e. Cisco, Symantec, Microsoft, Sophos, F5, Blue Coat, etc.) by simply plugging-in and adding a deeper layer of inspection, GDPR intelligent policies and adaptive security.

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
United Kingdom

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
Australia

Tel: +61 (0) 294 241 200
Technical Support: +61 2 9424 1200
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0) 221 8282 9888
Technical Support: +49 (0) 221 8282 9886
Email: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3) 5326 3470
Email: info.jp@clearswift.com

United States
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

Feature	Benefit
	Visibility
Data-at-rest discovery	Discover and mitigate critical information found on laptops, servers, network and cloud drives.
Data-in-motion monitoring and control	Monitor and control critical information in email and web traffic. Control through Adaptive Redaction, Encryption and blocking.
Data-in-use monitoring and control	Monitor and control removable media devices on endpoints. Encrypt or prevent copying to removable media, including USB sticks and CD / DVD ROMs.
Direction agnostic policies	Protect against potential inbound compliance issues as well as outbound ones.
	Adaptive Security
Inbound advanced threat protection	Information borne threats are neutralized before they become problems.
Outbound data leak protection	Prevent data leaks (inadvertent or malicious) across all communication channels (email, web & endpoint).
Adaptive Redaction	Automatically redact text from commonly used applications based on predefined keywords or tokens. Remove unwanted or sensitive file history information including custom and even "unexpected" (or rogue) properties. Detect active content and remove any traces of it.
Adaptive encryption	Multiple encryption methods based on context to communicate information securely.
	Intelligent Policy Enforcement
Flexible and granular policy controls	Easily define policies across multiple communication channels, giving consistency of discovery and flexibility of action to be taken.
Lexical analysis and regular expression rules	Search communication content for keywords and phrases using simple expressions or more complex pattern matching, with regular expressions, Boolean and locational searches to identify sensitive data patterns. Create custom tokens to enable more refined search profiles to reduce false positives and also check against Structured Data sources.
Cloud collaboration policies	Protect information sent to the cloud and received from it. Scan cloud drives for data-at-rest.
Binary file type identification	Accurate signature based identification with ability to define own file signatures prevents file spoofing.
File and sub-file information monitoring and governance	Register classified documents, monitor and control information at both file and sub-file levels across email and web egress points.
	Governance
Predefined governance dictionaries	Readily identify information required by GDPR, including credit card, bank account, social security, personal IDs and national security numbers. Fast time to implement.
Customizable reports	Easy to modify, run and share graphical reports with intuitive drill down suitable for all compliance officers as well as IT managers.
Full SMTP, HTTP & HTTP/S inspection and analysis	See inside encrypted traffic to prevent inbound and outbound sensitive data incidents.
Social media control including Facebook, LinkedIn, Twitter and YouTube	Allow access to Web 2.0 sites but only to content and features allowed by policy.
Active Directory (AD) and LDAP integration	Full user-based policy control for flexible policy and audit reporting by group or individual.
SNMP, SMTP and SYSLOG Alerting	SNMP or SMTP management alerts facilitates 'lights out' data center deployment and log files can be automatically consolidated using SYSLOG.

clearswift