GDPR Solutions from Skyhigh

How Skyhigh can help organizations conform to EU data protection legislation

GDPR data protection legislation comes into effect in May 2018, to regulate the collection and use of personal information on people living in the 28 countries that make up the European Union. This document describes how organizations can use Skyhigh technologies to review and manage cloud computing environments and conform to the regulation. It covers the technologies available for both sanctioned cloud services such as Office 365, Salesforce and Box and shadow cloud services.

GDPR legislation is a global law regarding data protection, as it covers any organization that has data on individuals living in the EU. Consultancy firm PwC issued a press release in January 2017, stating that 92% of companies in the United States said complying to GDPR is their top data protection priority (the full regulation is available to view here).

Skyhigh has published a detailed, 68-page e-book; "GDPR – An Action Guide for IT," to help organizations interpret the legislation and provide guidance on the actions that need to be taken. If you are unsure of the breadth of GDPR, the e-book is a good place to start.

GDPR AND CLOUD COMPUTING

In the GDPR, the organization that defines what and how data is collected is called the Data Controller. Data Controllers are ultimately responsible for all data protection, no matter where the data travels and who else accesses it. The Data Controller must therefore ensure that all subcontractors, outsourcers and cloud service providers have the necessary processes, procedures, technologies and have trained their teams to ensure data is controlled.

The GDPR has 99 articles and covers many forms of data risk. Being compliant takes a mix of knowledge, processes, policies and training, as well as data tracking, controlling, and user and device management, all coming from a "privacy first" IT philosophy.

This document should not be considered legal advice and can only address a part of the requirements to comply with GDPR. No technology on its own can deliver compliance as GDPR requires a whole-company approach including policies, procedures, training, legal agreements with partner companies and should be led by governance, risk and compliance groups.

SKYHIGH'S GDPR FUNCTIONALITY FOR SANCTIONED CLOUD SERVICES

The table below takes edited text from the regulation and compares the requirements with the services available from Skyhigh (alone or in conjunction with other network and security technologies). Please read the full regulation for the complete text.

Please note that not all of the capabilities listed below are available for all cloud services, as they may depend on the capabilities offered by the cloud service, for example the API controls made available. Contact Skyhigh for full information for your services.

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 5: (Overview) Principles relating to processing of personal data	Data shall be processed in a manner that ensures appropriate security of the personal data...	Skyhigh's solution is designed to meet security, compliance, and governance requirements; specifically, to protect against unauthorised access, accidental loss, destruction or damage of the data.	Reports to compliance teams should be part of the Skyhigh management cadence and policies designed together with the compliance team should be documented
Article 5: Principles relating to processing of personal data	The controller shall be able to demonstrate compliance with [above]	Skyhigh's documentation can be used to demonstrate compliance. The management system can show the policies enforced and reporting can show data flows to and from the cloud.	• Document policies • Show reporting capabilities • Show set up in GUI • Show data flows to and from the cloud
Article 24: Responsibility of the Controller	The controller shall implement appropriate technical … measures to ensure and demonstrate that the processing of data is performed in accordance with GDPR	Skyhigh can deliver policies to reduce risk of data loss to high risk cloud services, controls on traffic, data loss prevention, logging and reporting of cloud traffic (including IaaS) delivering technology for compliance.	• Define DLP and reporting to show policies for GDPR • Block access to shadow cloud with high GDPR Risk • Continuously review new services added • Report on data leaving EU/EEA (CSP data hosted outside)
Article 25: Data protection by design and default	...implement appropriate technical measures and … implement necessary safeguards into the processing	Implementing Skyhigh demonstrates that the organization has designed and deployed security measures for cloud computing. In addition to traffic controls, Skyhigh can report on unused names/passwords, user authorizations and control/manage access granted to external parties, such as by cloud storage directory sharing.	• Show integration with SAML/ SSO/LDAP • Demonstrate appropriate policies are the default • Report data anomalies • Set collaboration policies • Implement data collaboration policies and report on attempted breaches of those policies • Report on unused accounts • Report on unusual privileged user behaviour • General reporting on data access

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 25: Data protection by design and default	Obligation applies to … [data] accessibility	Skyhigh logs traffic and reports on data access to/from cloud services; by user and cloud service, optionally including details on file names and contents. These include access by internal employees together with links shared, and data going to and from external users. Skyhigh can enforce policies to ensure safe use of data and devices, such as geo-location rules, re-authentication, policies providing different access to data for managed and unmanaged devices. Skyhigh can force employee users to pass through a secondary security mechanism, such as cloud-based SSO services that will enforce access control rules and manage data accessibility.	Define cloud policies that are data protection by design and default. If in doubt, reduce cloud access. Set other policies and reports as defined to the right
Article 28: Processor	The controller shall use only processors providing sufficient guarantees … of this regulation	Skyhigh can block, control and report on external people and organizations that share access and data via cloud services. This allows management to reduce risk of data loss.	• Set policies for trusted cloud services • Use appropriate mix of cloud attributes • Review the attributes that are rolled up to GDPR Risk score and decide whether individual risks are too high for your personal data requirements. • Check for certifications such as ISO 27018 • Do not allow data to be uploaded to clouds claiming intellectual property ownership • Ensure full data flow logging is available or add on from Skyhigh. • Review security incident notification time of each cloud service

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 30: Records of processing activities	Each controller … shall maintain a record of processing activities	Skyhigh's advanced logging of all traffic by users and admins provides a record of processing activities; user access, data edited, uploaded or downloaded, links and files shared etc.	• Check full logging of data to/from cloud services is available, or add on with Skyhigh • Identify all cloud service provider organisations • Review data transfers outside EU/ EEA/"adequate" countries
Article 30: Records of processing activities	Transfers of data to a third country or international organisation …identify that organisation	Skyhigh's registry of service hosting sites allows management to see the third party cloud processors accessing data, as well as check their security stance and the countries that data is hosted in. Controls can be placed on data based on the country of the user accessing the data and/or the user's domain.	• Ensure full logging of data to/from cloud services • Identify cloud service provider organisations • Review transfer outside EU/ EEA/"adequate" countries
Article 30: Records of processing activities	A general description of the technical measures [deployed]	Skyhigh's security functionality is described in the user manuals, which together with other Skyhigh documentation, may be useful to demonstrate compliance. Full logging of user activity allows data controllers to track and report on recipients who have access to data.	Review and document Skyhigh policies and reporting, escalation and anomaly detection and review processes.
Article 32: Security of processing	Shall implement appropriate measures … confidentiality, integrity, resilience	Skyhigh's Data Loss Prevention (Smart DLP) technology can allow IT to scan and report (optionally, can also be used to inform user, notify administer, block, tombstone, quarantine, encrypt, and/or delete) data being shared in the cloud. Skyhigh can report on users with excessive administration rights and on standard user and system administrator behaviour.	• Add Skyhigh Smart DLP solutions to appropriate cloud services • Review when services were last breached and implement appropriate policies based on this. • Implement sharing/collaboration control • Review cloud services backup & restore capabilities.

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 32: Security of processing	Appropriate level of security ... [against] ... accidental, destruction, loss, alteration, unauthorised disclosure of or access to personal data	Skyhigh can block/allow external link/file sharing, or allow all together based on white-listed domains. Skyhigh logs all traffic to/from cloud services, and can block downloads to insecure devices, as well as restrict access to corporate instances of cloud services, like preventing simultaneous access to personal Office 365 instances. Skyhigh can also block downloads to unmanaged devices from cloud services, and enforce consistent policies across multiple cloud services from one interface. Skyhigh can integrate with digital rights management (EDRM) at a file level.	• Add Skyhigh Smart DLP solutions to appropriate cloud services • Review when services were last breached and implement appropriate policies based on this. • Implement sharing/collaboration control • Review cloud services backup & restore capabilities.
Article 33: Notification of data breach to authority	The controller shall ... not later than 72 hours ... notify the ... authority	Skyhigh's logging can highlight data anomalies, stop data transfers in motion, and report on actions that may have led to data loss as part of reporting to the Data Protection Authority	• Ensure data logging is available • Implement alerts on data anomalies • Set policies to control transfers & collaboration • Review your forensic capabilities to respond to any incidents • Report to regulator on measures taken
Article 33: Notification of data breach to authority	Describe nature of breach ... numbers concerned ... consequences	Skyhigh can enhance standard cloud reporting to have a complete record of actions, allowing a forensic examination of traffic to report on the breadth of a data loss incident.	• Ensure data logging is available • Implement alerts on data anomalies • Set policies to control transfers & collaboration • Review your forensic capabilities to respond to any incidents • Report to regulator on measures taken

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 33: Notification of data breach to authority	Measures taken to address breach … mitigate breach	Skyhigh implementation can be described to the authorities to show the measures taken to mitigate a data breach.	• Ensure data logging is available • Implement alerts on data anomalies • Set policies to control transfers & collaboration • Review your forensic capabilities to respond to any incidents • Report to regulator on measures taken
Article 34: Communication breach … to data subject	Shall communicate data breach to subject without delay	Skyhigh's logs are available on demand, allowing an investigation to evaluate the size and scope of a data breach quickly, and decide who, and how, to inform the data subjects.	• Ensure data logging is available • Implement alerts on data anomalies • Set policies to control transfers & collaboration • Review your forensic capabilities to respond to any incidents. • Review policy incident communication plan.
Article 34: Communication breach … to data subject	Shall not be required if … data unintelligible … such as encryption.	Skyhigh's Smart DLP capability can encrypt files within cloud services with customer-managed and hosted keys, reducing risk of data loss. However, there is often a loss of functionality when encryption is added, so it is not effective in all situations.	• Consider Skyhigh encryption of traffic before sending to the cloud
Article 35: Data protection impact assessment	In particular, when using new technologies … carry out risk assessment of the impact … including measures to address the risks	Skyhigh's security technologies provide measures to reduce the risk of processing personal data and report on the risk level of the service. On-demand scans of cloud services (total files or new/changed) for personal data can help assess the ongoing risks.	• Review individual cloud services using all attributes • Perform cloud DLP scans to continuously monitor risks on all services • Implement IaaS services security capabilities • Constantly review new services being added to the portfolio

Article	GDPR Text	How Skyhigh Can Help	Actions Required
Article 45: Transfers [to a third country] based on adequacy	Transfers to third country only if commission has decided … ensures an adequate level of protection	Skyhigh can report on data transfers for third-party processors with data centres based in countries NOT on the EU 'adequate' list. Skyhigh tracks and reports on data storage and processing location country allowing the customer to review whether data is stored in questionable countries. Skyhigh can also deny downloads from cloud services to users by country.	• Review all cloud services with data outside EU/EEA/adequate countries using Skyhigh cloud service attributes • Keep reviewing data storage location watching for changes • Review legal basis of all data transfers
Article 46: Transfers subject to appropriate safeguards	Binding corporate rules, standard data protection clauses or enforceable commitments	Skyhigh can report on third-parties accessing data via cloud services so that the legal department can check the contracts in place with those third-parties.	• Skyhigh Cloud Service attributes include US Data Privacy Shield & data location • Report on new services for legal department to check legal basis for transfer

ADDITIONAL CLOUD CONTROLS

Skyhigh has functions to manage your cloud computing installation that are not directly demanded by GDPR. These provide a comprehensive set of security and management capabilities to further control and manage the cloud services in use.

DATA UPLOAD & DOWNLOAD INFORMATION

The reports provided by Skyhigh can include the name and type of files uploaded to the cloud to help investigate possible data breaches. If a user accesses or downloads an unusual amount of data from a cloud service and then uploads that data to another service in a short time period it may indicate an exfiltration attempt.

DATA LOSS PREVENTION (DLP) INTEGRATION

Skyhigh can incorporate its own Smart DLP technology or integrate with existing on-premises DLP services to review data using existing DLP schemas. Data can be scanned for personal content as it is uploaded to the cloud service or on-demand scans can be run on historical data already stored in the cloud.

SMART DLP

Skyhigh can define custom policies including Boolean logic, to define keyword validation rules with proximity (e.g. "name" within x words of "Date of birth") and regular expressions. Skyhigh can enforce policies based on document fingerprints in OneDrive, SharePoint Online and other cloud services. Skyhigh can implement

policies based on fingerprinting of both structured and unstructured data and supports policies based on third-party classification tags. Policies can be differentiated by user or department.

DLP REMEDIATION AND REPORTING

Smart DLP supports multi-tier remediation based on the severity of an incident. Compliance reviewers can rollback an automated remediation action (quarantine/restore) and apply a manual remediation action. DLP reporting includes pertinent data (e.g. user, file name, policy violated, path, collaborators) and the review interface, providing an excerpt of the content that triggered the violation.

PRIVILEGED USER MONITORING

Skyhigh can report on admin user actions to ensure that the organization doesn't have too many admin users with high-levels of access, and can watch admin users for inappropriate data access.

COMPLIANCE OF CLOUD SERVICE PROVIDERS

Skyhigh's registry includes a wealth of information on the technical and privacy standards supported by each cloud provider, such as ISO 27001, ISO 27018, SOC2, SOC3, PCI, HIPAA. With visibility into these certifications, organizations can decide which third-party services hook into Office 365, Box or Salesforce.com to support and enable their users.

REVERSE-PROXY & API DEPLOYMENT

For employees, Skyhigh redirects sanctioned clous access for both managed and unmanaged devices through the Skyhigh reverse proxy, allowing controls to be inserted on data in motion. For data sharing with third-parties via the cloud, Skyhigh uses the APIs from the CSPs to review and manage data out of band.

INFECTED DEVICES & FILES

Skyhigh can detect malware in file-sharing and collaboration services. Though Skyhigh does not directly inspect devices for infections, the system may recognize the actions of an infected device from its usage behavioral patterns. This can alert IT admins to a possible infection and take remedial actions.

ADVANCED THREAT PROTECTION - HIGH-RISK TRAFFIC PATTERNS

High-risk traffic patterns indicative of insider threats, external and privileged user threats can be detected by Skyhigh's user behaviour analytics technology and remedial actions can be taken.

The threat engine can be sensitively tuned to react on multi-event threats to reduce false positives through adjustments of machine learning models providing real-time previews of the impact on your actual dataset. To help investigate possible threats an audit trail of previous use activity can also be shown. Additionaly, Skyhigh integrates event data from third-party threat feeds, and can send threats to a SIEM for further investigation.

CONTEXTUAL ACCESS CONTROL

Access controls can be based on multiple parameters simultaneously, for example:

- Personal or corporate instances of Office 365
- Managed/unmanaged devices (EMM, certificate check)
- Activity (upload/download)
- Agent (Zscaler integration)
- SAML expressions

The actions taken include allow, block, view-only, force authentication, check device certificate, redirect, register DRM as well as others.

STRUCTURED DATA ENCRYPTION

Skyhigh provides multiple encryption technologies based on the requirements of the solution, all with enterprise control of the encryption keys.

- Field-level encryption
- Format preserving encryption
- Search preserving encryption
- Sort preserving encryption

ONGOING CHANGE

Threats to data are never static. As such, in a constantly evolving field, Skyhigh's solutions are always watching for new threats and unusual traffic patterns, while our solution's functionality is continuously updated to add additional enterprise security capabilities.

SKYHIGH'S GDPR FUNCTIONALITY FOR SHADOW CLOUD SERVICES

Skyhigh's global CloudTrust™ registry contains risk ratings for over 20,000 cloud services, all of which are evaluated across 50 different assessment points, including a newly created a "GDPR Risk Rating," allowing customers to see the relative risk rating of each cloud service based on critical GDPR criteria. This allows the IT teams to share risk levels and ratings with their governance, risk and compliance teams and define policies based on individual GDPR risk levels.

If a provider is considered a high-risk, remedial action can be taken and Skyhigh can provide further advice on specific services:

- Blocking that provider
- Redirecting users to a lower-risk alternative
- Negotiating improved terms and conditions
- Adding cloud Data Loss Prevention (Smart DLP)
- Adding encryption before data is sent to the service
- Integration with Single-Sign-On (SSO) systems and providers
- Restricting external file-sharing
- Setting geo-location and granular access controls
- Adding user, admin and data activity logging

The GDPR risk attribute can also be combined with other Skyhigh attributes for advanced filtering, reporting, blocking and other remedial actions.

Below is a partial list of the attributes that are major influences on the overall GDPR risk score.

Attribute	Values of concern
Data retention on termination of contract	Anything other than immediate deletion is cause for concern, as once your contract has ended, you can't be sure what the provider will do with your data.
Allows anonymous use	Any provider allowing anonymous use could be a source of data leak without knowing who has collected the data, making it impossible to use forensics to find the culprits, and investigate and report to the regulator.
Security Incident notification	Needs to be below < 1 day, otherwise data controller cannot fulfill the 72-hours notification to regulator.
Data location	Should not be hosted in a questionable country, unknown or undefined. Of minor concern is being hosted outside the EU, EEC or 11 countries considered "adequate" for privacy laws by the EU.
Admin activity logging	Should not be "no" or "unknown."
User activity logging	Should not be "no" or "unknown."
Data activity logging	Should not be "no" or "unknown."
IP ownership	Should not be "unknown", "undefined" or "SP owns."
Privacy policy	Should not be "unknown", "undefined" or "shares with 3rd party without customer agreement."
Overall GDPR-readiness score	Blended attribute taking into account 24 specific attributes, weighting them for importance in GDPR and scoring the results – between 1 and 9 – (scores of 7, 8, 9 should be investigated).

There are additional attributes that have a smaller influence on the overall GDPR risk score, and include items such as: data content type, granular access controls, seven different encryption and key management attributes, auto-sync of data, DLP integration, identity federation, IP filtering and various certifications.