VARONIS

GETTING READY FOR THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

Tips to Keep Your Unstructured Data in Compliance

1. Minimize Data Collection: The proposed EU law has strong requirements that limits the data companies collect from consumers.

- The less data, the less risk there is that hackers will expose sensitive data.
- **Before asking a consumer for data, carefully review what the data will be used for and determine whether less data points can achieve the same goal.**

2. Prompt Data Breach Reporting: Data breach notification is a new requirement for which EU companies will be responsible. Thr proposed new law says that companies should provide some initial breach details to the Data Protection Agency (DPA) within 24 hours and no later than 72 hours. The information should include the data that was exposed and the number of subjects that were affected.

- This means companies will have to be diligent about monitoring activity of their file data, such as reviewing system logs and audit trails.

- However, OS' generally can't handle the type of granular file monitoring and reporting that would be required for the EU. **A company will need special purpose-built software to watch its file system.**

3. Retain Carefully: The new law's minimization rules apply not only to the scope of the data collected but also how long it's kept.

This will lead to many questions about where the data is, when it was last accessed, and who owns it. Every file system has 'stale' data—rarely or never accessed information. So how can you find it?

Data governance software will be able to reach file activity and can tell you which data to keep, which to delete, and which to archive to long-term storage.

4. New Definition of Personal Identifier: These identifiers have traditionally been, for example, name, address, account number, and phone number. **The new EU definition says it is any data alone or in combination with other associated data that can be used to identify a person by using reasonable means.**

Not only does the law encompass traditional identifiers, but also IP and email addresses, biometric, and even geo-location, and other geographic data. This change is important because the EU law centers on protecting these identifiers. The Internet Age has created new ways to link data back to consumers.

To comply with the proposed EU law, companies will have to adjust file search filters to match the patterns of these non-traditional identifiers, and then check that appropriate access rights for the files containing these identifiers are enforced.

5. Clear Language:

- Companies will need explicit consent—an 'opt-in' from the consumer—when collecting data.

- The company must disclose the reason the data is being asked for, the retention period of the data, and the name of the external data processor if one is used.

6. Erase Button: Data privacy is a fundamental right—it's in the EU Charter. At the same time though, the 'right to be forgotten' has caused some controversy for Internet search companies over the years.

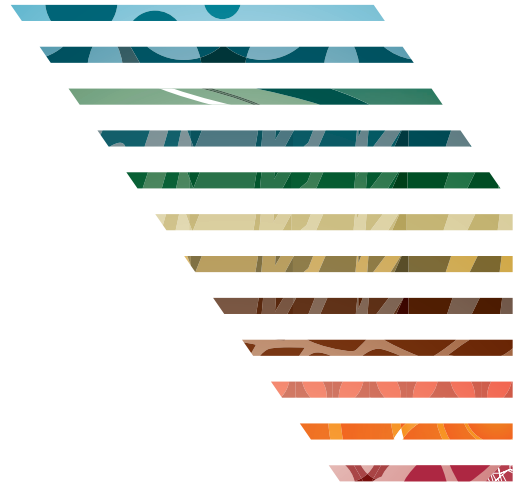
But there's also a less controversial and related 'right to erasure.' It means that when consumers withdraw consent on data they've given, the companies will have to remove it. The right to erasure also applies to data that has reached its retention period.

This means that when asked by a consumer, companies will have to remove all of the data that's been collected—and that includes data in spreadsheets, documents, and emails.

7. Whither the Cloud? When companies decide to process data in the cloud, they'll have to get assurance that their provider has the required security measures in place. Their contract will require that any data collected by the provider will have to be handed back at termination of the service.

Bottom line: Companies can't avoid the EU law by outsourcing data to the cloud. The EU law still follows the data.

ENGLISH: www.varonis.com
DEUTSCH: www.varonis.de



VARONIS

GUT GERÜSTET FÜR DIE EU GENERAL DATA PROTECTION RULE (GDPR)

Tipps für die Compliance von unstrukturierten Daten

1. Datensparsamkeit–Begrenzen Sie die Datenerfassung: Die vorgeschlagenen EU-Gesetze beinhalten strenge Anforderungen an Unternehmen und limitieren das Erfassen von Verbraucherdaten gemäß dem Grundsatz der Datensparsamkeit.

- Je weniger Daten gesammelt werden, desto geringer ist das Risiko, sensible Daten einem Hackerangriff auszusetzen.
- **Bevor Sie Daten erheben, sollten Sie sich bewusst machen wozu Sie diese Daten im Einzelnen benötigen, und entscheiden ob Sie nicht auch mit weniger Daten das gleiche Ziel erreichen.**

2. Anzeigepflicht bei Datenschutzverletzungen: Die Anzeige-beziehungsweise Berichtspflicht bei Datenschutzverletzungen ist eine neue gesetzliche Anforderung, der europäische Unternehmen Folge leisten müssen. Sie sind verpflichtet, erste Details zu einer Datenschutzverletzung innerhalb von 24 Stunden, spätestens innerhalb von 72 Stunden, der Data Protection Agency (DPA) zu melden, einschließlich von Informationen dazu, welche Daten und Bereiche betroffen sind.

- Das heißt, Unternehmen müssen sämtliche Dateiaktivitäten sorgfältig überwachen wie beispielsweise System-Logs und Audit Trails.
- Allerdings stellen Betriebssysteme ein derart granulares Monitoring und Reporting wie es die EU-Gesetzgebung fordert im Allgemeinen nicht zur Verfügung. **Dazu bedarf es speziell entwickelter Software-Tools, die Dateiaktivitäten dahingehend überwachen.**

3. Sorgfältig aufbewahren: Die neue Gesetzgebung bezieht sich nicht nur auf das Erfassen, sondern auch auf das Speichern von Daten und darauf wie lange sie gespeichert werden. Damit gehen wesentliche Fragen einher: Wo genau sind diese Daten gespeichert, wann wurde zuletzt darauf zugegriffen und wer ist der eigentliche Eigentümer der Daten? In praktisch jedem Dateisystem gibt es veraltete Daten. Informationen, auf die selten bis gar nicht mehr zugegriffen wird. Wie finden Sie diese Daten?

Dazu benötigen Sie eine Data-Governance-Software, die sämtliche Dateiaktivitäten nachvollzieht, und die Ihnen sagt, welche Daten Sie aufbewahren, welche Sie löschen und welche Sie langfristig speichern sollten.

4. "Persönliche Kennung" neu definiert: Zusätzlich hat die EU die Definition der persönlichen Kennung erweitert. Zu diesen persönlichen Kennungen zählten bisher beispielsweise Name, Adresse, Konto- oder Telefonnummern. **Die neue Definition geht deutlich darüber hinaus: Sie besagt, dass dazu alle Daten gehören, allein oder in Kombination mit anderen, die als personenbezogene Daten geeignet sind die Identität einer Person unter Anwendung angemessener Methoden festzustellen.**

Das Gesetz umfasst sowohl die traditionellen Personenkennzeichen als auch IP- und E-Mail-Adressen, biometrische Daten und sogar geolokalisierte Informationen und weitere geografische Daten.

Diese Erweiterung ist besonders bedeutsam, weil sich die neue EU-Gesetzgebung darauf konzentriert, diese persönlichen Kennungen beim Datenschutz in den Mittelpunkt zu stellen. Das Internet-Zeitalter hat neue Mittel und Wege geschaffen, um Daten zurückzuverfolgen und eindeutig mit den jeweiligen Nutzern in Verbindung zu bringen.

Um dieser veränderten EU-Gesetzeslage Rechnung zu tragen, müssen Unternehmen die im Dateisystem verwendeten Suchfilter an die erweiterten Kennzeichnungsschemata anpassen. Anschließend müssen die Zugriffsrechte für diejenigen Dateien überprüft und gestärkt werden, die solche personenbezogenen Daten und Kennzeichen enthalten.

5. Eindeutige Sprachregelungen:

- Wenn Sie Nutzerdaten erfassen wollen, brauchen Sie die ausdrückliche Zustimmung des Nutzers, das bekannte "opt-in".
- Zudem muss das jeweilige Unternehmen offenlegen aus welchem Grund die Daten erfasst werden, wie lange die Daten gespeichert werden und den Namen eines gegebenenfalls beteiligten externen Datenverarbeitungsunternehmens.

6. Die "Löschen"-Funktion: Die Vertraulichkeit von Daten ist ein fundamentales Recht, das in der EU-Charta festgeschrieben wurde. Gleichermaßen hat das sogenannte "Recht auf Vergessen" unter den verschiedenen Suchmaschinen-anbietern über Jahre hinweg eine kontroverse Diskussion ausgelöst.

Weniger kontrovers, aber damit verbunden ist "das Recht auf Löschung" von Daten. Das bedeutet, wenn ein Nutzer seine vormals gegebene Einwilligung zum Nutzen und Speichern seiner Daten zurückzieht, ist das betreffende Unternehmen verpflichtet diese Daten zu löschen. Das Recht auf Löschung gilt auch dann, wenn die Speicherfrist bereits erreicht ist.

Ja, genau: Das heißt, wenn ein Benutzer ein Unternehmen darauf anspricht, hat dieses Unternehmen sämtliche Daten zu löschen, die erfasst worden sind. Dazu zählen Daten in Tabellen, Dokumenten und E-Mails.

7. Wohin mit der Cloud? Haben sich Unternehmen dazu entschlossen Daten innerhalb der Cloud zu verarbeiten, müssen sie sicherstellen, dass der Provider die entsprechenden Datenschutzrichtlinien umsetzt. Zwischen Kunde und Provider muss vertraglich festgelegt sein, dass sämtliche vom jeweiligen Provider erfassten Daten an den Kunden zurückgehen wenn das Vertragsverhältnis erlischt.

Fazit: Unternehmen können sich dem neuen EU-Gesetz nicht entziehen, indem sie Daten in die Cloud auslagern. Auch hier folgt das Gesetz den Daten.