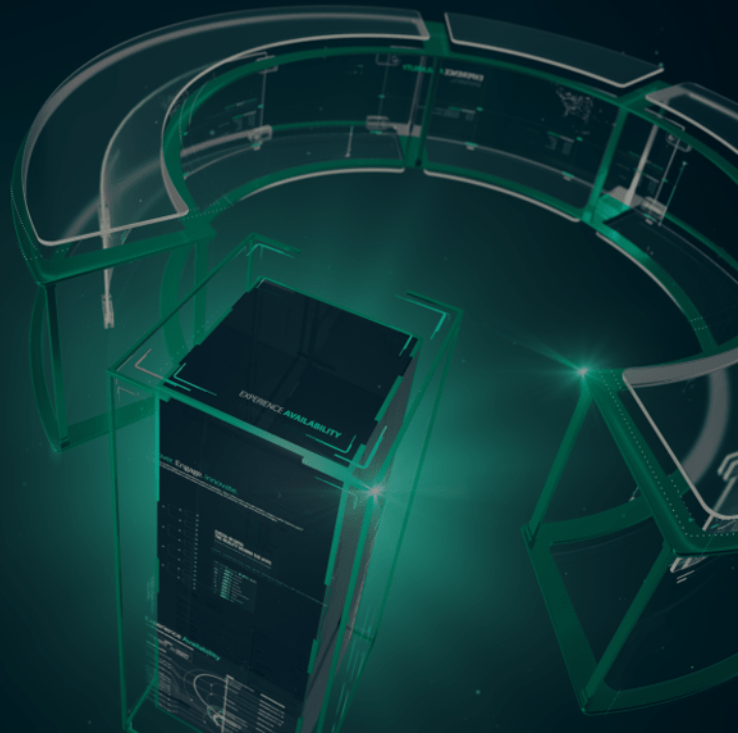
Veeam & GDPR megfelelőség



Varsányi András
Veeam Systems Engineer
Hungary

GDPR - *General Data Protection Regulation*

- "The proposed new EU data protection regime extends the scope of the EU data protection law to all foreign companies processing data of EU residents. It provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 2% of worldwide turnover."

- A szabályozás szöveges változatának megjelenése: 2016.04.27.

- Életbelépés időpontja: 2018.05.25

- Hivatalos „segédlet" az alkalmazás módjáról: ???

GDPR – Legfontosabb alapfogalmak

- **Scope** – „data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU.” **Fontos kivétel**: „The regulation does not purport to apply to the processing of personal data for national security activities or law enforcement within the European Union.”

- **Responsibility and accountability** – „the data controller should implement measures which meet the principles of data protection by design and data protection by default.”

- **Consent**

- **Data Protection Officer (DPO) -** „managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data…understanding legal compliance with data protection laws and regulations.”

GDPR – Legfontosabb alapfogalmak

- **Pseudonymisation** – „a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information.”

- **Data breaches** – „must be reported to the Supervisory Authority within 72 hours after having become aware of the data breach. Individuals have to be notified if adverse impact is determined.” **Fontos kivétel: „data processor or controller do not have to notify the data subjects if anonymized data is breached.”**

- **Sanctions**

- „a warning in writing in cases of first and non-intentional non-compliance,

- regular periodic data protection audits,

- a fine up to 10000000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, or a fine up to 20000000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.”

GDPR – Legfontosabb alapfogalmak

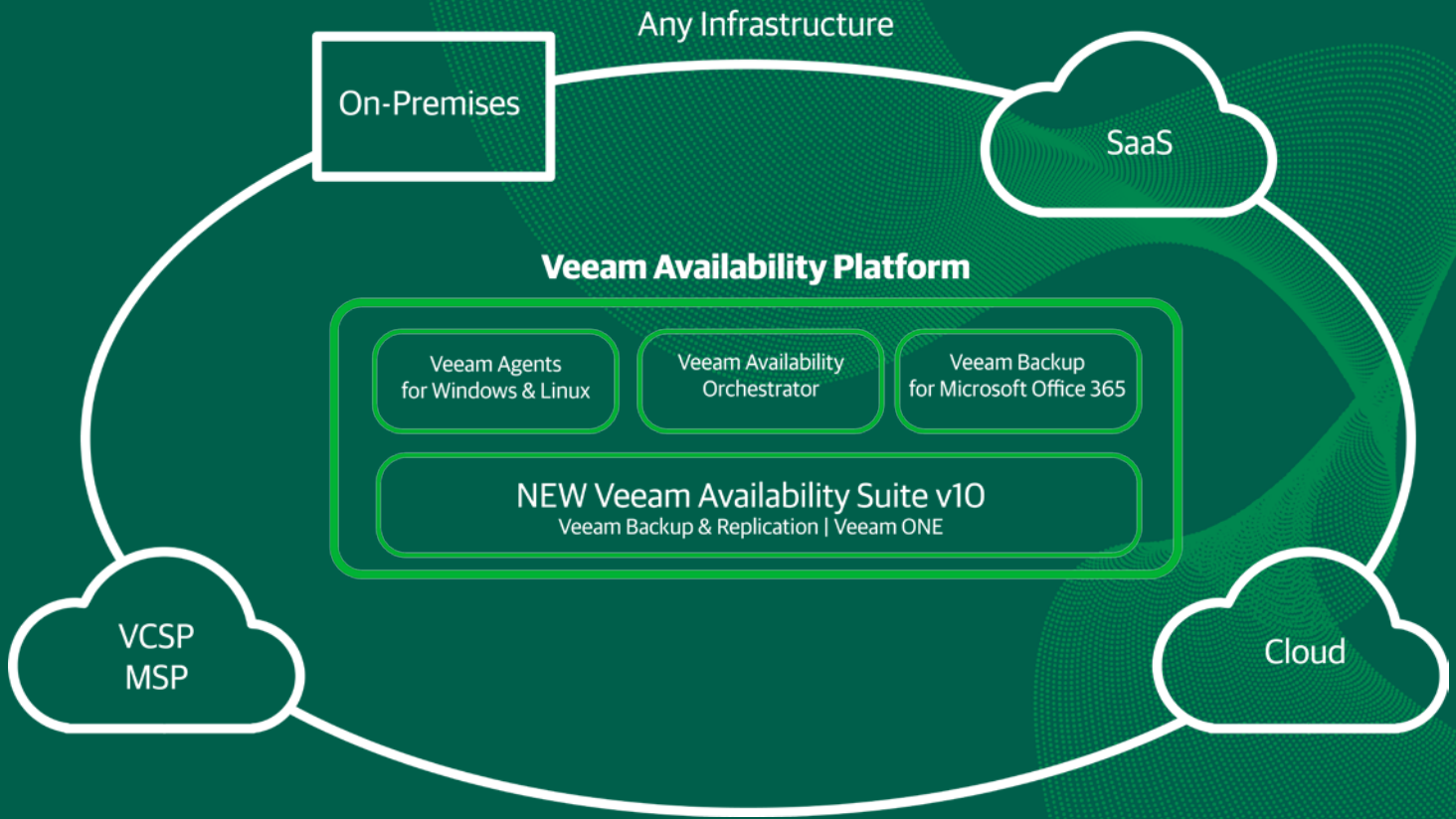
- **Right to erasure (eredetileg „Right to be forgotten”)** – „the data subject has the right to request erasure of personal data related to them on any one of a number of grounds including non-compliance with article 6.1 (lawfulness) that includes a case (f) where the legitimate interests of the controller is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.”

- **Data portability -** „A person shall be able to transfer their personal data from one electronic processing system to and into another, without being prevented from doing so by the data controller.

- **Data protection by Design and by Default – „**requires that data protection is designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default…

GDPR – Legfontosabb alapfogalmak

- **Records of processing activities** – „Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request


Any Infrastructure
On-Premises
SaaS
Veeam Availability Platform
Veeam Agents for Windows & Linux
Veeam Availability Orchestrator
Veeam Backup for Microsoft Office 365
NEW Veeam Availability Suite v10
Veeam Backup & Replication | Veeam ONE
VCSP MSP
Cloud

GDPR + Veeam – *Mire NEM alkalmas?*

- A Veeam NEM egy automatizált „GDPR Officer”
- NEM ad „GDPR-Certified” pecsétet
- NEM egy „GDPR Compliancy Engine”

GDPR + Veeam – *Mire alkalmas?*

- **Az adatok láthatósága (Data Visibility) -** A Veeam Availability Suite használatával a felhasználók rendkivül informativ betekintést nyerhetnek az erőforrásokkal, SLA-val (data retention policy) és megfelelőséggel (compliancy) kapcsolatos adataikba.

- **Az adatnövekedés kontrollja (Handle Data Growth)** - A Veeam Availability Suite-alapú megoldás könnyedén skálázható a növekvő igényekkel összhangban, és számos olyan beépitett mechanizmussal rendelkezik, amelyek segitenek a mentések/archivumok szükségtelenné vált adatainak eltávolitásában.

- **Automatizáció (Automation) -** Az újonnan keletkező adatok és az újonnan létrejött workloadok számos, előzetesen meghatározott parameter alapján automatikus védelemben részesülhetnek, ezáltal biztositva az adatok mindenkori helyreállithatóságát akár betörések, ransomware támadások és egyéb rosszindulatú külső, vagy belső tevékenységek esetén is.

GDPR + Veeam – *Mire alkalmas?*

- **Titkositás (Encryption)** - A GDPR előirásainak megfelelően az adatok kezelőjének pontos információkkal kell rendelkeznie arról, hogy az adatok hol találhatóak, mi az esetleges mozgásuk iránya, és kik férnek hozzájuk. A Veeam által kinált többféle (köztük „end-to-end” jellegü) titkositási metódus révén az üzemeltetők biztosak lehetnek afelől, hogy az adatokhoz -függetlenül attól, hogy azok „nyugalmi” állapotban vannak-e, vagy pedig mozgásban- csak az arra ténylegesen felhatalmazott személyek férnek hozzá.

- **Indexing / e-Discovery** - A Veeam Availability Suite automatikus guest OS indexálása és számos különböző workload számára elérhető e-Discovery megoldása az adatokat rendkivül könnyen lokalizálhatóvá teszi.

GDPR + Veeam – *Gyakorlati példák*

- **Ténylegesen is vissza tudom állitani az adataimat?**

- (Hivatkozva a GDPR 25. cikkelyére - Article 25: „Data Protection by design and by default”) A kérdéses követelmény könnyedén teljesithető a Veeam beépitett SureBackup és SureReplica technologiáinak használatával, amelyek lehetővé teszik az üzemeltetők által kijelölt rendszerek helyreállithatóságának tesztelését – akár automatikusan, akár manuálisan, mindezt egy predefiniált & izolált virtuális laboratóriumban. A kérdéses tesztekről készült riportok szükség esetén egyértelmüen bizonyithaják, hogy a kérdéses adatok helyreállithatóak.

- Mindezeken túl a Veeam ONE felügyeleti szoftverkomponens monitorozási/analitikai és riportolási megoldásai az előzetesen meghatározott SLA-k ellenőrzésében is képesek segitséget nyújtani (pl. felhivni az üzemetetők figyelmét az SLA-nak nem megfelelő, védtelen adatforrásokra).

GDPR + Veeam – *Gyakorlati példák*

- **Ki fért hozzá az adataimhoz?**

- A helyreállitási (restore) tevékenységek kivétel nélkül naplózásra kerülnek, valamint riportok nyerhetőek belőlük, amelyek egyértelmüen bizonyithatják, hogy ki, mikor, milyen adatot és hová állitott helyre.

- **Adat-életciklus felügyelet (Data Retention)**

- (Hivatkozva a GDPR 25. cikkelyére - Article 25: „Data Protection by design and by default”). A Veeam lehetővé teszi az üzemeltetők számára, hogy a megfelelő mechanizmusokat használják annak érdekében, hogy az adatokat csak az azok specifikus igényei által diktált időtartamra tartsák meg. Ezen mechanizmusok többek közt magukba foglalják a GFS szabályozást (Grandfather-Father-Son, széleskörüen alkalmazott data retention policy), a visszaállitási pontok számának meghatározhatóságát és nyomonkövetésüket az adatok teljes életciklusa alatt, amelyek együttesen biztositják, hogy a szükségtelenné vált adatok nem kerülnek erőforrásigényes újrafedolgozásra, hanem a szabályzattal összhangban törlődnek (vagy off-site megőrzésre kerülnek).

GDPR + Veeam – *Gyakorlati példák*

- **„A felejtés joga” (Right to be forgotten)**

- (Hivatkozva a GDPR 17. cikkelyére - Article 17: „Right to be forgotten”). A kérdéses szabályozás elsősorban a produktiv adatokra vonatkozik, vagyis nem ir elő olyasfajta korlátozást, miszerint olyan adatokat kellene törölni, amelyek különben törvényi, vagy egyéb szabályozási okokból kifolyólag továbbra is életbevágóan szükségesek, és mentésekben vagy archivált állományokban kerültek tárolásra. A Veeam két módon képes segiteni a 17. cikkelynek való megfelelőséget:

- A guest OS fájl indexing technológia használatával az adatok abból a meghatározott lokációból nyerhetőek vissza, ahol a mentések biztonságos módon tárolódnak. Az eljárás nemcsak strukturálatlan adatokhoz alkalmazható, hanem a Veeam Explorer technológia eDiscovery képességeinek alkalmazásával akár levelezési állományokra is

- A Veeam Virtual Lab technológia segitségével az adatok egy bizonyitottan izolált „karanténban” vizsgálhatóak meg egy esetleges helyreállitást megelőzően

GDPR + Veeam – *Gyakorlati példák*

- **Végpont-végpont titkositás (End-to-end encryption)**

- Végpont-végpont jellegü titkositás elsősorban akkor vállhat szükségessé, ha az adatok országhatárok közötti transzferjét végezzük – különösképp igaz mindez az Európai Unió határain kivülre történő adattranszferekre. A Veeam „end-to-end” titkositást képes biztositani mind a „nyugalmi” állapotban lévő (data at rest), mind az aktiv transzfer alatt álló (data in-flight) adatokra.

- **Az adatok elérhetőségének helyreállitása (Restore the availability of data)**

- (Hivatkozva a GDPR 32. cikkelyére - Article 32: „The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”) A Veeam megoldás lehetővé teszi az adatok elérhetőségének rendkivül gyors helyreállithatóságát adatszivárgások, betörések, adatmegsemmisülés, RansomWare támadások, egyéb rosszindulatú tevékenységek és előre nem látható incidensek esetén. Egy egyszerü Veeam mentés több mint 50 féle különböző visszaállitási lehetőséget biztosit, amelyek lehetővé teszik az adatok elérhetőségének gyors, egyszerü és biztonságos helyreállithatóságát.

GDPR + Veeam – *Gyakorlati példák*

- **Végpont-végpont titkositás (End-to-end encryption)**

- Végpont-végpont jellegü titkositás elsősorban akkor vállhat szükségessé, ha az adatok országhatárok közötti transzferjét végezzük – különösképp igaz mindez az Európai Unió határain kivülre történő adattranszferekre. A Veeam „end-to-end” titkositást képes biztositani mind a „nyugalmi” állapotban lévő (data at rest), mind az aktiv transzfer alatt álló (data in-flight) adatokra.

- **Az adatok elérhetőségének helyreállitása (Restore the availability of data)**

- (Hivatkozva a GDPR 32. cikkelyére - Article 32: „The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident”) A Veeam megoldás lehetővé teszi az adatok elérhetőségének rendkivül gyors helyreállithatóságát adatszivárgások, betörések, adatmegsemmisülés, RansomWare támadások, egyéb rosszindulatú tevékenységek és előre nem látható incidensek esetén. Egy egyszerü Veeam mentés több mint 50 féle különböző visszaállitási lehetőséget biztosit, amelyek lehetővé teszik az adatok elérhetőségének gyors, egyszerü és biztonságos helyreállithatóságát.

GDPR + Veeam – *Gyakorlati példák*

- **A hozzásférés szabályozása (Access Control)**

- (Hivatkozva a GDPR 25. cikkelyére - Article 25: „Access Control”) Az RBAC-alapú felügyelet használatával a Veeam megnyugtatóan képes biztositani azt, hogy a felhasználók csak azon adatokhoz férhetnek hozzá, amelyek ténylegesen szükségesek feladataik elvégzéséhez. Az RBAC egyaránt alkalmazható a napi tevékenységekre és a visszaállitási folyamatokra. Az ezekről történő riportolási képesség tovább növeli a hozzáférés kontrolljának hatásfokát.

- **Az adatok exportja (Export of data)**

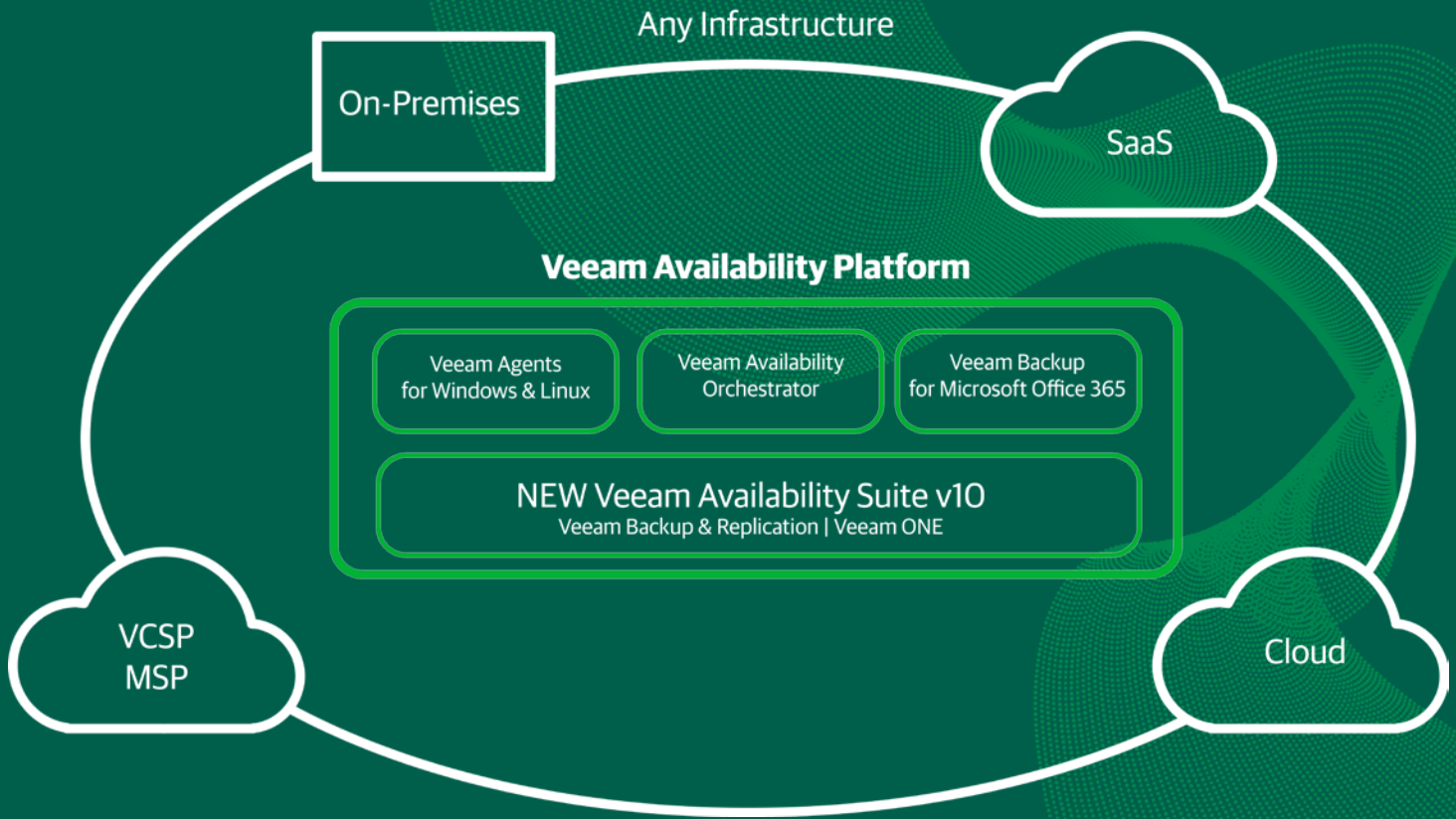
- (Hivatkozva a GDPR 15. cikkelyére - Article 15: „Right of access by the data subject”) A Veeam lehetővé teszi az adatok exportját számos széleskörüen elterjedt formátumban, amely biztositja, hogy az adatok tulajdonosa akár a saját -nem vállalati- rendszerein is hozzáférhessen azokhoz.

GDPR + Veeam – *Gyakorlati példák*

- **Az adatok védelme (Protect data, wherever it resides)**

- A Veeam biztositja az adatok védelmét, függetlenül attól, hogy azok on-premise, hibrid, vagy akár publikus felhőben kerültek tárolásra. Az adatok on-premise tárolókba történő mentésével lehetővé válik azok lokális felkutatása, helyreállitása és vizsgálata – a mindenkori igényekkel összhangban.

DEMO


Any Infrastructure
On-Premises
SaaS
Veeam Availability Platform
Veeam Agents for Windows & Linux
Veeam Availability Orchestrator
Veeam Backup for Microsoft Office 365
NEW Veeam Availability Suite v10
Veeam Backup & Replication | Veeam ONE
VCSP MSP
Cloud

Köszönjük a figyelmet!