

Continuitatea afacerii si General Data Protection Regulation

Pregateste-ti solutia de Backup & Disaster Recovery



Despre GDPR

Acest nou Regulament, **GDPR - Regulation (EU) 2016/679**, a fost adoptat la **27 aprilie 2016** si va intra in vigoare la **25 mai 2018**. Este un regulament prin care Parlamentul European, Consiliul European si Comisia Europeana **intentioneaza sa consolideze si sa unifice protectia datelor pentru persoanele fizice in cadrul Uniunii Europene**.

Inlocuieste actuala directiva a Uniunii Europene privind datele cu caracter personal, cunoscuta ca *Directive 95/46/EC* adoptata in 1995.

Regulamentul va trebui respectat de fiecare organizatie a statelor UE si orice organizatie care detine date cu caracter personal referitoare la persoanele din Uniunea Europeana va fi obligata sa isi revizuiasca procesele de gestionare a informatiilor.

Prin introducerea de principii noi cum este "dreptul de a fi uitat" si obligatii de notificare, in anumite circumstante, o companie este obligata sa stearga in totalitate datele cu caracter personal intr-o anumita perioada de timp daca un utilizator o cere.

De asemenea persoanele afectate de o incalcare a datelor personale trebuie sa fie notificate fara intarziere daca orice informatie cu caracter personal s-a scurs catre destinatari neautorizati si aceasta scurgere prezinta o amenintare grava la drepturile si libertatile persoanelor respective.



Ce inseamna GDPR pentru tine si afacerea ta?

In Uniunea Europeana exista un set de legi pentru colectarea si prelucrarea datelor personale. Oricine colecteaza sau proceseaza date personale are obligatia sa le protejeze prin respectarea si aplicarea legilor in vigoare. In momentul de fata aceasta fiind noul set GDPR.

Aceste legi se aplica datelor fizice si electronice?

Da. Noile legi GDPR se aplica atat datelor electronice (precum email sau data de baze) cat si documentelor fizice care contin astfel de date. Asta inseamna ca avem o responsabilitate sa pastram in siguranta si sa distrugem orice documente care pot contine date sensibile.

Ce vor avea companiile de facut?

Da. Orice organizatie va trebui sa implementeze masuri tehnice si organizationale pentru procesarea datelor intr-un mod corespunzator. Pentru a stabili nivelul necesar de securitate, trebuie luat in calcul riscul prezentat de procesarea si colectarea datelor, in special in cazuri de accident sau pierdere. Ar trebui sa se poata arata masurile care au fost luate pentru a tine datele confidential.

Este importanta protectia datelor?

Foarte importanta. Siguranta datelor trebuie inclusa in toate procesele operationale. Companiile trebuie sa puna la punct toate procesele prin care se prelucreaza datele, sa se colecteze si prelucreze doar cele necesare.

Ce este de facut?

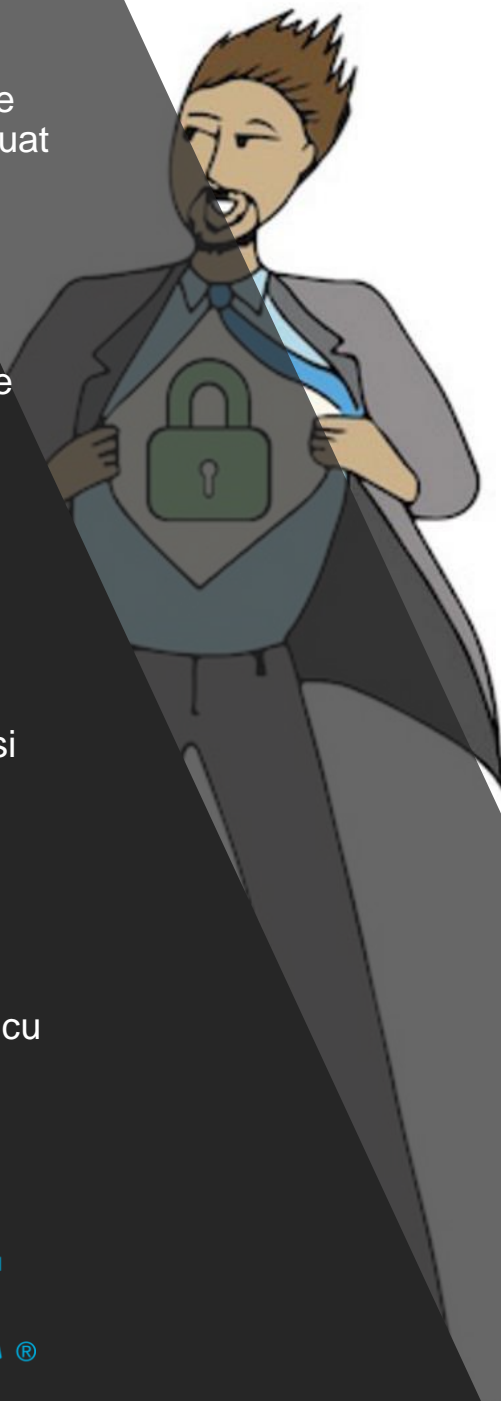
Pentru a deveni o companie care se afla in parametrii GDPR, este nevoie de un plan si un buget de resurse (incluzand IT). De asemenea, trebuie luat in calcul ca exista un termen limita pentru implementare. Mai jos regasiti cateva activitati cu care puteti incepe:

Plan de impact al sigurantei datelor personale, impreuna cu o harta a circuitului de informatii in companie.
Revizuiti toate contractele, mai ales pe cele care contin transferul de date personale.

Update la sistemul de gestionare a informatiilor care include documente detaliate privind preluarea si prelucrarea datelor confidentiale.
Verifica toate datele actuale acumulate, si verifica daca ai nevoie sa le folosesti.

Sistem de distrugere a informatiilor de care nu ai nevoie.
Asigura-te ca: consimtamantul, dreptul de a fi uitat, portabilitatea datelor si dreptul la obiectie sunt asigurate de companie prin proceduri si politica firmei.

Creaza un sistem de notificare a erorilor de sistem care pot afecta persoanele de la care s-au acumulat date.
Desemneaza un responsabil cu Protectia Datelor, un DPO
Training, Training, Training, pentru toate persoanele care intra in contact cu aceste date.
Stabileste controale regulate pentru a identifica si solutiona posibile probleme.



Inainte de a "cumpara" o solutie de recuperare a datelor, este necesar sa iti faci temele.

Trebuie sa defisesti foarte clar nevoile afacerii tale.

Stabileste obiectivele timpului de recuperare.

RTO indica cat de rapid ai nevoie sa iti recuperezi datele in urma unui dezastru.

Trebuie sa fii foarte specific, nu este suficient sa spui "ASAP" sau "imediat". Gandeste-te la fiecare server si calculator si intreaba-te "cat de critic este pentru tine?", "cat de repede ai nevoie ca acel backup sa fie restaurat?"
Tine minte: Daca acel endpoint nu este critic pentru tine, nu iti pierde timpul si resursele (banii) sa il aduci inapoi.

STEP 1

Stabileste obiectivele punctelor de recuperare.

RPO indica perioada maxima pe care o poti suporta fara acces la datele tale in urma unui dezastru

Intreaba-te simplu:

Cat de multe date esti dispus sa pierzi?
Ce date vor fi cele mai costisitoare si dificil de recreat?

Astfel veti stii ce date trebuie sa fie acoperite de backup cat mai des. Din nou, nu fi tentat sa spui ca totul este vital! Nu toate datele din organizatia ta sunt egale!

Step 2

Cum arata o solutie performanta de recuperare in caz de dezastru?

Copiile de rezerva reprezinta fundatia oricarei solutii de recuperare in cazul unui dezastru. In orice caz, nu toate copiile de rezerva sunt la fel. Tine minte:

- A. Tehnologia bazata pe imagini s-a dovedit a fi de cea mai buna clasa, tehnologia veche de scriere pe banda s-a dovedit a fi nedemna de incredere.
- B. Posibilitatea sa faci copii de rezerva atat de des precum doresti (indicat la fiecare 15 minute pentru datele critice)
- C. Verificarea rapida si usoara a copiilor de rezerva
- D. O solutie care poate sa iti faca backup la intregul mediu IT/ forta de munca, inclusiv pentru angajatii de pe teren, orice aplicatie software as a service pe care o utilizezi (Office 365, G Suites).
- E. Copiile de rezerva nu sunt conectate la retea de pe care se face backup.
- F. Solutia pe care o alegi trebuie sa suporte toate platformele: Windows, Linux, atat masinile fizice cat si cele virtuale.

On / Off premise

Dupa ce ti-ai facut copiile de rezerva, ai nevoie de **un spatiu sigur de stocare** si de **accesul securizat** la acestea. Cea mai buna practica pe care noi o recomandam este ca prima data sa iti **stochezi** copiile de rezerva **local**, apoi sa le **replici** intr-o locatie **secundara**. Asta inseamna ca vei avea posibilitatea sa recuperezi foarte repede datele din locatie interna.

In orice caz, in situatia in care nu poti accesa locatiea ta interna, atunci ai optiunea sa iti restaurezi copiile din locatie externa, de fapt, continuitatea business-ului este garantata atunci cand ai un backup in afara locatiei tale.

Cateva lucruri pe care sa le ai in vedere atunci cand cauti o solutie de backup si disaster recovery:

1. Este backup-ul meu local scalabil?
2. Pot sa fiu flexibil in ceea ce priveste perioadele de backup?
3. Pot sa imi replic datele intr-o anumita locatie la alegerea mea (intr-o locatie secunda a organizatiei), sau intr-un cloud public sau privat? Pot face replicarea la o anumita ora, convenabila mie?

StorageCraft Disaster Recovery Solution iti ofera versatilitatea sa iti construiesi propriul plan de recuperare in caz de dezastru indiferent de hardware-ul ales. Iti va oferi flexibilitate deplina sa iti setezi backup-urile in functie de programul tau.



Testeaza backup-ul!

Trebuie sa ai posibilitatea sa iti testezi planul de recuperare in cazul unui dezastru! Nu ii permite dezastrului sa fie primul tau test!

Un plan bun o sa fie foarte usor de testat. Aceasta este singura modalitate prin care poti valida obiectivele timpului de recuperare.

StorageCraft Disaster Recovery iti permite sa testezi si sa verifici datele foarte usor, ori de cate ori iti doresti.



Recuperarea datelor

Poate parea evident, dar din pacate acesta este pasul unde multe solutii de **BDR** cedeaza. Solutia pe care o alegi trebuie sa iti permita **recuperarea** datelor tale **oricand si oriunde**.

Cand un **dezastru** de tipul **Ransomware** te loveste, trebuie sa ai incredere **100%** ca iti vei recupera datele si ca iti poti continua activitatea.

Tine minte urmatoarele intrebari:

Aceasta solutie va indeplini asteptarile mele pentru **RTO** si **RPO**?

Va functiona solutia aceasta de fiecare data?

Daca serverul meu cedeaza, il pot resatura pe o masina virtuala?

Dar viceversa?

Trebuie sa fac restaurarea pe acelasi hardware?

StorageCraft Recovery Solution ofera fiabilitate de viteza și flexibilitate pentru recuperare.



Concluzie

Numaratoarea inversa pana la **GDPR** a inceput. Companiile din Europa vor trebui sa se asigure ca sunt conforme pana in **Mai 2018**.

Implementarea unei soluții eficiente de recuperare în caz de dezastru este un prim pas important spre conformitate.

Continuitatea afacerii tale incepe aici. Asigura-te ca ai ales solutia potrivita de backup si disaster recovery!

Descopera solutiile [BDR StorageCraft!](#)

