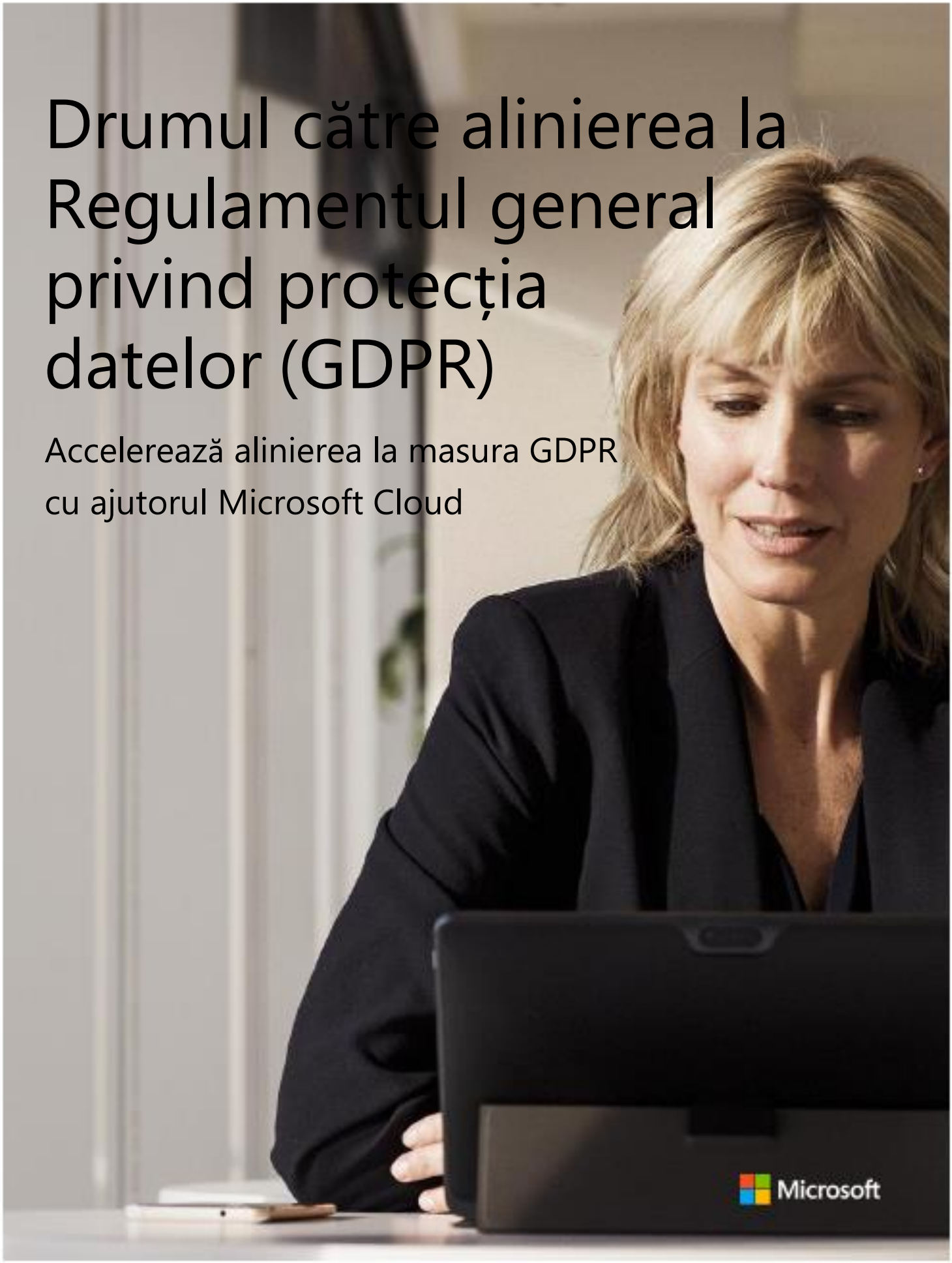
Drumul către alinierea la Regulamentul general privind protecția datelor (GDPR)

Accelerează alinierea la masura GDPR cu ajutorul Microsoft Cloud



Cuprins

Disclaimer

Acest material despre GDPR este modul cum Microsoft interpretează această masură, la data publicării. Am dedicat mult timp analizei GDPR, mai ales în a întelege intenția și sensul GDPR. Procesul de implementare însă este un process specific fiecărei companii și nu toate aspectele și interpretările GDPR sunt bine determinate.

Drept urmare, această carte albă este furnizată în scop informativ și nu trebuie să se considere că oferă consiliere juridică sau că determină modul în care GDPR ți se poate aplica ție sau organizației tale. Te încurajăm să colaborezi cu specialiști calificați pentru a discuta despre GDPR, despre modul în care se aplică organizației tale și despre cele mai bune moduri de asigurare a conformității.

MICROSOFT NU OFERĂ NICIO GARANȚIE EXPRESĂ, IMPLICITĂ SAU STATUTARĂ CU PRIVIRE LA INFORMAȚIILE DIN ACEAST MATERIAL. Aceast material este furnizat „ca atare”. Informațiile și opiniile exprimate în aceast document, inclusiv adresele URL și alte referințe la site-uri web de pe internet, se pot modifica fără notificare prealabilă.

Acest document nu îți oferă niciun drept legal de proprietate intelectuală asupra niciunui produs Microsoft. Poți copia și utiliza această carte albă doar în scopuri de referință internă.

Publicată în mai 2017

Versiunea 1.1

Introducere

Pe 25 mai 2018 va intra în vigoare o lege europeană privind confidențialitatea, care stabilește un nou standard global pentru drepturile la confidențialitate, securitate și conformitate.

Regulamentul general privind protecția datelor sau GDPR se referă, în esență, la protejarea și asigurarea drepturilor persoanelor la confidențialitate. GDPR stabilește cerințe globale de confidențialitate stricte, care guvernează modul în care sunt gestionate și protejate datele personale, respectându-se, în același timp, alegerile individuale – indiferent unde sunt trimise, procesate sau stocate datele.

Împreună cu clienții noștri depunem eforturi pentru a atinge obiectivele de confidențialitate ale GDPR. În cadrul Microsoft, noi credem că confidențialitate este un drept fundamental și că GDPR este o etapă importantă pentru clarificarea și asigurarea drepturilor persoanelor la confidențialitate. Recunoaștem, însă, de asemenea, că GDPR va necesita schimbări semnificative în organizațiile din întreaga lume.

Deși drumul spre alinierea la GDPR poate părea dificil, noi suntem aici pentru a te ajuta.

Angajamentul Microsoft față de GDPR

Încrederea stă la baza misiunii noastre de a oferi fiecărei persoane și organizații de pe planetă posibilitatea de a avea realizări mai mari. Avem o abordare bazată pe principii pentru dezvoltarea încrederii, cu angajamente clare față de confidențialitate, securitate, conformitate și transparență. Aplicăm aceste principii pe măsură ce ne pregătim pentru GDPR.

Înțelegem că responsabilitatea pentru conformarea cu GDPR este una comună. De aceea, ne-am angajat ca, la data începerii aplicării regulamentului, pe 25 mai 2018, să fim în conformitate cu GDPR în serviciile noastre cloud.

De asemenea, suntem dedicați împărtășirii experienței noastre cu regulamentele complexe, pentru a te ajuta să folosești cea mai bună modalitate prin care organizația ta să îndeplinească cerințele de confidențialitate ale GDPR. Cu cel mai cuprinzător set de oferte de conformitate și securitate pus la dispoziție de un furnizor de soluții cloud și cu un vast ecosistem de parteneri, suntem pregătiți să te sprijinim în inițiativele tale de confidențialitate și securitate, acum și în viitor.

Ca parte a angajamentului nostru de a-ți fi parteneri pe drumul spre aliniearea la GDPR, am dezvoltat această material pentru a te ajuta cu pregătirile. Documentul oferă o prezentare generală a GDPR, descrie ce vom face pentru a ne pregăti pentru GDPR și furnizează exemple de măsuri pe care le poți lua astăzi împreună cu Microsoft pentru a-ți începe propriul drum spre conformarea cu GDPR.

Așteptăm cu nerăbdare să împărtășim noi informații despre modul în care te putem ajuta să te conformezi cu această importantă lege nouă și, pe parcurs, să îmbunătățești protecția confidențialității personale. Vizitează secțiunea GDPR a Centrului de autorizare Microsoft pentru a găsi resurse suplimentare și pentru a afla mai multe despre modul în care Microsoft te poate ajuta să îndeplinești cerințe specifice din GDPR.

Înțelegerea GDPR – elemente de bază

Înainte să descriem modurile specifice în care Microsoft te poate ajuta să te pregătești pentru GDPR, am dori să răspundem la unele dintre cele mai importante întrebări cu privire la regulament și la ceea ce poate însemna pentru tine. O prezentare generală mai extinsă poate fi găsită aici.

Ce este GDPR?

Regulamentul general privind protecția datelor este un nou regulament privind confidențialitatea în Uniunea Europeană. Acesta oferă oamenilor control suplimentar asupra datelor personale, asigură transparența cu privire la utilizarea datelor și impune securitate și mijloace de control pentru protejarea datelor.

GDPR se aplică organizației mele?

GDPR se aplică la scară mai largă decât poate părea la prima vedere. Legea impune noi reguli pentru companii, agenții guvernamentale, organizații non-profit și alte organizații care oferă bunuri și servicii oamenilor din Uniunea Europeană (UE) sau care colectează și analizează date legate de rezidenții UE. GDPR se aplică indiferent unde sunteți localizat.

Spre deosebire de legile privind confidențialitatea din alte jurisdicții, GDPR se aplică organizațiilor de orice dimensiune și din orice domeniu. UE este privită adesea la nivel internațional ca model în ceea ce privește chestiunile legate de confidențialitate, de aceea ne așteptăm ca, în timp, anumite concepte din GDPR să fie adoptate și în alte părți ale lumii.

Când intră în vigoare GDPR?

GDPR intră în vigoare pe 25 mai 2018. Va înlocui Directiva existentă privind protecția datelor (Directiva 95/46/CE), care este în vigoare din 1995. GDPR a devenit, de fapt, o lege în UE în aprilie 2016, dar, având în vedere schimbările semnificative pe care unele organizații vor trebui să le facă pentru a respecta regulamentul, s-a inclus și o perioadă de tranziție de doi ani.

Care sunt conceptele cheie din GDPR?

GDPR este structurat în jurul a șase principii:

- Necesitatea transparenței cu privire la gestionarea și utilizarea datelor cu caracter personal.
- Limitarea procesării datelor cu caracter personal la scopurile specificate, legitime.
- Limitarea colectării și stocării datelor cu caracter personal la scopurile declarate.
- Oferirea posibilității persoanelor vizate de a corecta sau solicita ștergerea datelor cu caracter personal.
- Limitarea stocării datelor cu caracter personal doar la perioada necesară atingerii scopului

declarat.

- Asigurarea protecției datelor cu caracter personal prin practici de securitate adecvate.

Exemple de cerințe GDPR cu privire la aceste principii

- Conform GDPR, persoanele au dreptul să știe dacă o organizație le procesează datele cu caracter personal și să înțeleagă scopurile respectivei procesări. O persoană are dreptul de a solicita ștergerea sau corectarea datelor, de a cere să nu mai fie procesate, de a refuza marketingul direct și de a revoca consimțământul pentru anumite utilizări ale datelor sale. Dreptul de portabilitate a datelor oferă persoanelor dreptul de a muta datele în altă parte și de a primi asistență în acest sens.
- GDPR impune organizațiilor să securizeze datele cu caracter personal în conformitate cu sensibilitatea acestora. În cazul unei breșe de securitate, controlorii de date trebuie să notifice autoritățile corespunzătoare în decurs de 72 de ore. În plus, dacă breșa va duce la apariția de riscuri mari pentru drepturile și libertățile persoanelor, organizațiile vor trebui, de asemenea, să notifice fără întârziere persoanele afectate.
- Pentru procesarea datelor cu caracter personal trebuie să existe o bază legală. Consimțământul pentru procesarea datelor cu caracter personal trebuie să fie „oferit în mod liber, specific, informat și lipsit de ambiguități". Conform GDPR, există cerințe de consimțământ unice pentru protejarea copiilor.
- Organizațiile trebuie să evalueze impactul asupra protecției datelor, pentru a anticipa impactul proiectelor asupra confidențialității și pentru a lua măsuri, după cum este necesar. Trebuie menținute înregistrări ale activităților de procesare, consimțăminte pentru procesarea datelor și conformitatea cu GDPR.
- Conformitatea cu GDPR nu este o activitate care are loc o singură dată, ci este un proces continuu. Neconformarea cu GDPR poate duce la amenzi semnificative. Pentru a asigura conformitatea cu GDPR, organizațiile sunt încurajate să implementeze o cultură de confidențialitate, pentru a proteja interesele persoanelor cu privire la datele cu caracter personal.

Pentru o prezentare generală mai detaliată a GDPR și pentru a înțelege mai bine termeni precum pseudonimizare, procesare, controlere, procesatori, subiecți ai datelor și date cu caracter personal, vizitează Microsoft.com/GDPR. Dorim să te ajutăm să îndeplinești cerințele GDPR și să sprijini în continuare dreptul persoanelor la confidențialitate.

Asocierea cu Microsoft pe drumul către GDPR

Alinierea la GDPR este o provocare pentru toate companiile. Va necesita timp, instrumente,

procese și expertiză și poate cere schimbări semnificative în practicile de gestionare a confidențialității și datelor. Drumul tău către conformarea cu GDPR va fi mai ușor dacă utilizezi un model de servicii cloud bine structurat și dacă implementezi un program eficient de administrare a datelor. În ceea ce privește succesul conformării cu GDPR, te poți baza pe Microsoft și pe ecosistemul nostru extins de parteneri.

Microsoft are un istoric lung de furnizare a unor servicii cloud pe care te poți baza. Avem o abordare bazată pe principii față de confidențialitate, securitate, conformitate și transparență, cu angajamente solide, pentru a ne asigura că poți avea încredere în tehnologia digitală pe care te bazezi. Avem cel mai extins portofoliu de conformitate din domeniu și am fost primii care am adoptat standarde cheie, precum standardul de confidențialitate a serviciilor cloud ISO/IEC 27018. Clienții și partenerii noștri beneficiază de experiența extinsă pe care o avem în ceea ce privește confidențialitatea, securitatea, conformitatea și transparența.

Pe măsură ce te pregătești de conformarea cu GDPR, iată la ce altceva te poți aștepta din partea noastră:

- **Tehnologie pe măsura nevoilor tale.** Poți să profiți de portofoliul nostru extins de servicii cloud enterprise, pentru a-ți îndeplini obligațiile GDPR privind aspecte precum ștergerea, rectificarea, transferul, accesarea și refuzarea procesării datelor cu caracter personal. Mai mult, te poți baza pe ecosistemul nostru global extins de parteneri pentru asistență specializată, atunci când utilizezi tehnologiile Microsoft.
- **Angajamente contractuale.** Te susținem prin angajamente contractuale pentru serviciile noastre cloud, care includ asistență promptă de securitate și notificări în conformitate cu noile cerințe GDPR. În martie 2017, acordurile noastre de licențiere cu clienții pentru serviciile cloud Microsoft vor include angajamente de conformitate cu GDPR în momentul în care începe punerea în aplicare.
- **Împărtășim experiența.** Îți vom spune cum a fost drumul nostru către conformitatea cu GDPR, pentru ca tu să poți adapta lucrurile pe care noi le-am învățat, cu scopul de a alege cel mai bun drum pentru organizația ta.

Introducere în GDPR

O abordare de platformă a GDPR

Sistemele pe care le utilizezi pentru a crea, stoca, analiza și gestiona date pot fi răspândite în mai multe medii IT – dispozitive personale, servere locale, servicii cloud, chiar și Internet of Things. Aceasta înseamnă că este posibil ca mare parte din resursele tale IT să facă obiectul cerințelor GDPR.

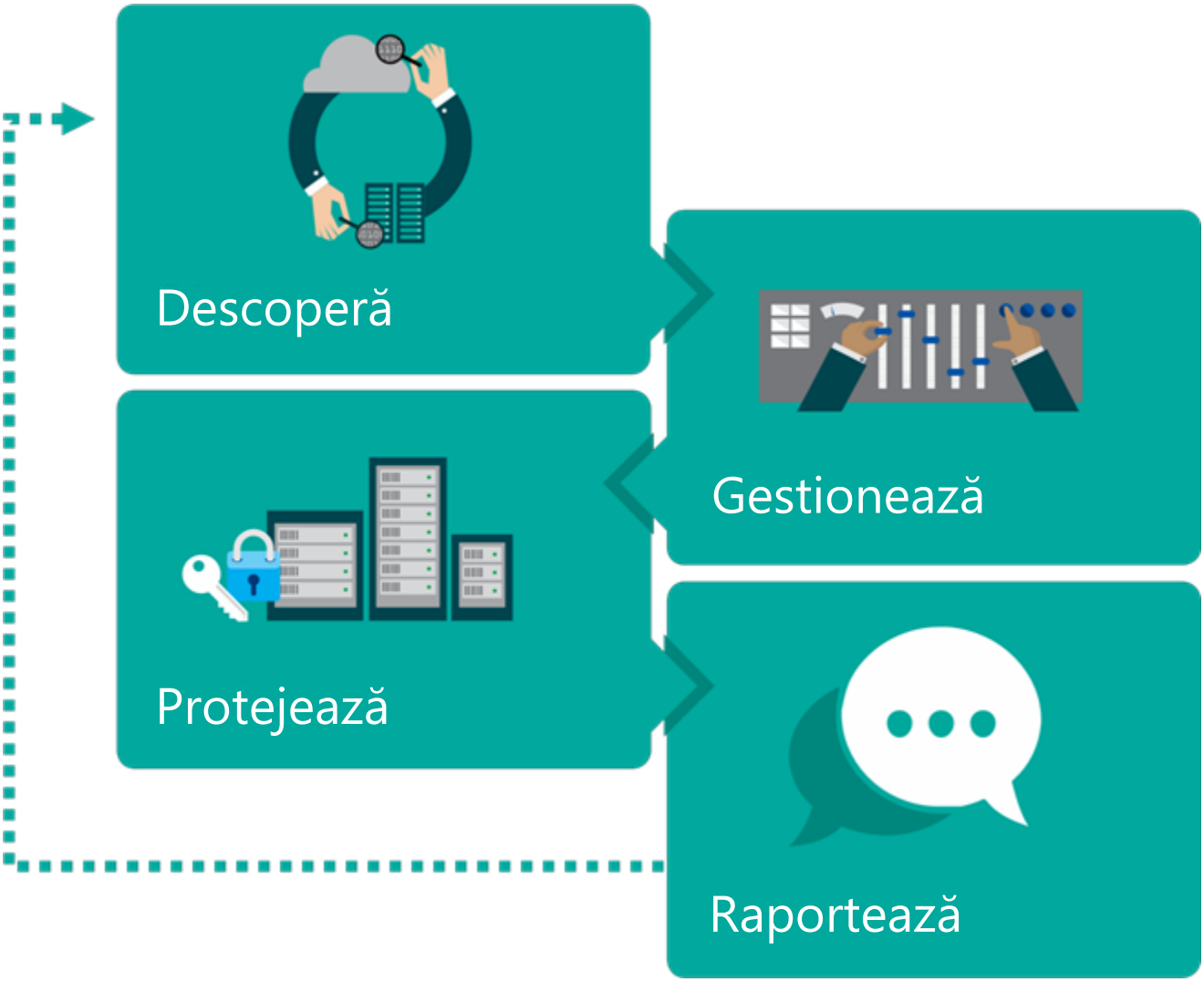
Eforturile tale de a te conforma cerințelor GDPR vor fi utilizate cel mai bine prin studierea

cerințelor în mod holistic și în contextul tuturor obligațiilor legale și de reglementare cu privire la confidențialitate. De exemplu, multe dintre controalele de securitate pentru prevenirea, detectarea și abordarea vulnerabilităților și breșelor de securitate cerute de GDPR sunt similare cu cele impuse de alte standarde de protecție a datelor, precum standardul de confidențialitate a serviciilor cloud ISO 27018.

În loc să monitorizezi controalele cerute de standardele sau reglementările individuale de la caz la caz, o practică mai bună este să identifici un set general de controale și capacități pentru a satisface aceste cerințe. În mod similar, în loc să evaluezi tehnologiile și soluțiile individuale în raport cu o reglementare extinsă precum GDPR, abordarea de platformă – cum ar fi una compusă din Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure și Dynamics 365 – poate oferi o perspectivă mai clară pentru a asigura nu doar alinierea la GDPR, ci și cu alte cerințe importante.

Îți recomandăm să începi drumul către conformitatea cu GDPR concentrându-te pe patru pași cheie:

- **Descoperă –** identifică ce date cu caracter personal deții și unde sunt localizate.
- **Gestionează –** administrează modul în care sunt utilizate și accesate datele cu caracter personal.
- **Protejează –** implementează controale de securitate pentru a preveni, detecta și răspunde la vulnerabilități și breșe de securitate.
- **Raportează –** dă curs solicitărilor de date, raportează breșele de securitate și păstrează documentația necesară.



Pentru fiecare dintre pași, am evidențiat exemple de instrumente, resurse și caracteristici în diferite soluții Microsoft care pot fi utilizate pentru a te ajuta să abordezi cerințele din pasul respectiv. Acest document nu este un manual de instrucțiuni complet, de aceea am inclus linkuri prin intermediul cărora poți afla mai multe detalii. De asemenea, poți găsi informații suplimentare la adresa Microsoft.com/GDPR.

Având în vedere cât de multe măsuri trebuie luate, nu ar trebui să aștepți începerea aplicării GDPR pentru a te pregăti. Ar trebui să revizuiești acum practicile de confidențialitate și gestionare a datelor.

Următoarele secțiuni evidențiază elemente specifice din fiecare componentă a GDPR și descriu moduri în care poți utiliza produse și servicii disponibile astăzi de la Microsoft pentru a începe.

la măsuri astăzi

Descoperă: identifică ce date cu caracter personal deții și unde sunt localizate

Primul pas către alinierea GDPR este să evaluezi dacă această măsură se aplică organizației tale și, dacă da, în ce măsură. Această analiză începe prin a înțelege ce date deții și unde sunt localizate.

GDPR se aplică datelor mele?

GDPR reglementează colectarea, stocarea, utilizarea și partajarea de „date cu caracter personal". Datele cu caracter personal sunt definite foarte larg în GDPR ca fiind *orice* date asociate unei persoane fizice identificate sau identificabile.

Dacă organizația ta deține astfel de date – în baze de date de clienți, în formulare de feedback completate de clienți, în conținut de e-mailuri, în fotografii, în înregistrări CCTV, în înregistrări ale programelor de fidelitate, în baze de date de resurse umane sau în orice altă parte – sau dorește să le colecteze și dacă datele aparțin sau sunt asociate rezidenților UE, atunci trebuie să te conformezi GDPR. Reține că datele cu caracter personal nu trebuie să fie stocate în UE pentru a fi sub incidența GDPR – GDPR se aplică datelor colectate, procesate sau stocate în afara UE dacă sunt asociate rezidenților UE.

Efectuarea inventarului

Pentru a înțelege dacă GDPR *se aplică* organizației tale și, dacă da, ce obligații impune, este important să inventariezi datele din organizația ta. Aceasta te va ajuta să înțelegi ce date au caracter personal și să identifici sistemele în care sunt colectate și stocate datele, să înțelegi de ce au fost colectate, cum sunt procesate și partajate și cât de mult sunt păstrate.

Iată câteva exemple de modalități specifice prin care ofertele noastre de soluții cloud și soluții locale te pot ajuta în primul pas către GDPR.

Azure

Având în vedere că Azure este o platformă cloud deschisă și flexibilă, acesta include un serviciu prin care sursele de date pot fi descoperite și identificate mai ușor. Catalogul de date Microsoft Azure este un serviciu cloud administrat complet, care servește drept sistem de înregistrare și sistem de descoperire pentru sursele de date ale organizației. Cu alte cuvinte, Catalogul de date Azure te ajută să descoperi, să înțelegi și să utilizezi surse de date pentru a valorifica mai bine datele existente. După ce o sursă de date este înregistrată în Catalogul de date Azure, metadatele acesteia sunt indexate de serviciu pentru ca tu să poți căuta și descoperi cu ușurință datele de care ai nevoie.

Dynamics 365

Dynamics 365 furnizează mai multe capacități de vizibilitate și auditare care pot fi utilizate prin intermediul tablourilor de bord Raportare și Analiză din Dynamics 365 cu scopul de a identifica datele cu caracter personal:

- Dynamics 365 include un Asistent raport pe care îl poți utiliza pentru a crea cu ușurință rapoarte, fără să utilizezi interogări bazate pe XML sau SQL.
- Tablourile de bord din Dynamics 365 furnizează o prezentare generală a datelor de afaceri – informații care te ajută să identifici acțiuni și care pot fi vizualizate în toată organizația.
- Microsoft Power BI este o platformă de business intelligence (BI) cu autoservire pe care o utilizezi pentru a descoperi, analiza și vizualiza date și pentru a partaja aceste perspective sau pentru a colabora cu colegii pentru a le îmbunătăți.

Suita Enterprise Mobility + Security (EMS)

Enterprise Mobility + Security include tehnologii de securitate bazate pe identitate care te ajută să descoperi, să controlezi și să protejezi datele cu caracter personal deținute de organizația ta, precum și să descoperi potențialele probleme ascunse și să detectezi breșele de securitate.

Microsoft Cloud App Security este un serviciu cuprinzător care furnizează o vizibilitate superioară, controale extinse și o protecție îmbunătățită pentru date în aplicațiile cloud. Poți observa ce aplicații cloud sunt utilizate în rețea – identificând peste 13.000 de aplicații de pe toate dispozitivele – și poți beneficia de evaluări de riscuri și analize continue.

Microsoft Azure Information Protection te ajută să identifici care sunt datele sensibile și unde sunt localizate. Poți să cauți date marcate cu o anumită sensibilitate sau poți să identifici în mod inteligent datele sensibile atunci când este creat un fișier sau un e-mail. După identificare, poți clasifica și eticheta automat datele – toate acestea în baza politicii dorite a companiei.

Office 365

Există câteva soluții Office 365 specifice care te ajută să identifici sau să gestionezi accesul la datele cu caracter personal:

- Prevenirea pierderii datelor (DLP) din Office și Office 365 poate identifica peste 80 de tipuri comune de date sensibile, inclusiv date financiare, date medicale și informații de identificare personală.
- Căutarea de conținut din Centrul de securitate și conformitate Office 365 poate căuta în cutii poștale, foldere publice, grupuri Office 365, Microsoft Teams, site-uri SharePoint Online, locații din One Drive pentru business și conversații din Skype for Business.

- Căutarea din Office 365 eDiscovery poate fi utilizată pentru a găsi text și metadate în conținut din activele tale Office 365 – SharePoint Online, OneDrive pentru business, Skype for Business Online și Exchange Online.
- Office 365 Advanced eDiscovery, bazat pe tehnologiile de învățare programată, te poate ajuta să identifici documente care sunt relevante pentru un anumit subiect (de exemplu, o investigație de conformitate) în mod rapid și cu o precizie mai bună decât căutările tradiționale de cuvinte cheie sau verificarea manuală a unor cantități mari de documente. Advanced eDiscovery poate reduce în mod semnificativ costurile și eforturile pentru a identifica relații dintre date și documente relevante prin utilizarea învățării programate, pentru a instrui sistemul să exploreze în mod inteligent seturi mari de date și să identifice rapid ceea ce este relevant - reducând datele înainte de revizuire.
- Guvernarea avansată a datelor utilizează informații și perspective asistate de computer pentru a te ajuta să găsești, să clasifici, să stabilești politici și să iei măsuri pentru a gestiona ciclul de viață al datelor care sunt cele mai importante pentru organizație.

SharePoint

Poți utiliza Serviciul de căutare SharePoint pentru a căuta funcționalități în cadrul aplicației, cu scopul de a găsi date cu caracter personal. Pentru a identifica și căuta conținut sensibil, SharePoint Server 2016 oferă aceleași capacități de prevenire a pierderii datelor precum Office 365.

SQL Server și Bază de date SQL Azure

Limbajul SQL poate fi utilizat pentru a interoga baze de date și pentru a particulariza instrumente sau servicii care pot contribui la îndeplinirea acestei cerințe. Căutarea este acceptată în întregime prin interogări, însă înregistrarea completă a urmăririi trebuie executată la nivel de aplicație. Activitatea Script furnizează codul pentru execuția de funcții particularizate, cum ar fi interogările complexe de date care nu sunt disponibile în activitățile și transformările integrate pe care le furnizează SQL Server Integration Services. Activitatea Script poate, de asemenea, să combine funcții într-un singur script în loc să utilizeze activități și transformări multiple. Această suită de produse include și o funcționalitate puternică de business intelligence care oferă utilizatorilor finali acces la perspectivele asupra datelor.

Windows și Windows Server

Pentru a găsi date în Windows, poți utiliza Windows Search pentru a urmări și localiza datele cu caracter personal pe computerul local și pe orice dispozitive conectate pentru care ai permisiuni de acces adecvate. Pentru a îmbunătăți capacitățile Windows Search de a localiza datele țintă, poți configura Opțiunile de indexare din Panoul de control pentru a particulariza capacitățile Windows Search (de exemplu prin indexare conținutului fișierelor).

Gestionează: administrează modul în care sunt utilizate și accesate datele cu caracter personal

GDPR furnizează subiecților datelor - persoane asociate datelor - mai mult control cu privire la modul în care datele lor cu caracter personal sunt capturate și utilizate. Subiecții datelor pot, de exemplu, să solicite ca organizația ta să partajeze datele asociate lor, să le transfere datele către alte servicii, să corecteze erorile din datele lor sau să restricționeze procesarea anumitor date în cazuri specifice. În unele cazuri, aceste solicitări trebuie trimise în perioade de timp fixe.

Guvernarea datelor

Pentru a îți îndeplini obligațiile față de subiecții datelor, va trebui să înțelegi ce tipuri de date cu caracter personal procesează organizația ta, în ce mod și în ce scopuri. Inventarierea datelor discutată anterior este un prim pas către acest lucru. După ce inventarierea este finalizată, este, de asemenea, important să dezvolți și să implementezi un plan de guvernare a datelor. Un plan de guvernare a datelor te poate ajuta să definești politici, roluri și responsabilități pentru accesul, gestionarea și utilizarea datelor cu caracter personal și te poate ajuta să te asiguri că practicile de gestionare a datelor se conformează cu GDPR. De exemplu, un plan de guvernare a datelor poate oferi organizației tale încrederea că respectă efectiv solicitările subiecților datelor de a șterge sau transfera datele.

Servicii cloud Microsoft

Pentru a sprijini strategia de guvernare a datelor, serviciile cloud Microsoft sunt dezvoltate prin metodologiile Microsoft Privacy-by-Design și Privacy-by-Default. Atunci când îți încredințezi datele către Azure, Office 365 sau Dynamics 365, rămâi unicul proprietar: reții dreptul, titlul și interesul pentru datele stocate în servicii.

Serviciile cloud Microsoft iau măsuri solide pentru a te ajuta să protejezi datele clienților împotriva accesului inadecvat sau a utilizării de către persoane neautorizate, după cum se detaliază în Centrul de autorizare Microsoft. Aceste măsuri includ restricționarea accesului de către personalul și subcontractorii Microsoft și definirea atentă a cerințelor pentru a răspunde la solicitarea datelor clienților de către instituțiile guvernamentale.

Totuși, poți să accesezi datele propriilor clienți în orice moment și cu orice motiv.

În plus, redirecționăm solicitările de date ale instituțiilor guvernului pentru a ți se adresa direct, în afara cazului în care acest lucru este interzis prin lege și am contestat pe cale oficială încercările instituțiilor guvernamentale de a interzice dezvăluirea unor astfel de solicitări.

Pentru a ne asigura că serviciile cloud Microsoft sunt gestionate corect și pentru a furniza asigurări clienților, serviciile cloud sunt auditate cel puțin anual în baza câtorva standarde globale de confidențialitate a datelor, inclusiv HIPAA și HITECH, CSA Star Registry și câteva standarde ISO. Aceste rapoarte pot fi accesate la adresa https://servicetrust.microsoft.com/Documents/ComplianceReports.

Pe lângă aceste angajamente, îți vom furniza controlul necesar pentru a verifica modul în care sunt gestionate datele și cine are acces la date specifice din organizație.

Azure

Azure Active Directory este o soluție de gestionare a identității și accesului în cloud. Gestionează identitățile și controlează accesul la Azure, local, și la alte resurse, date și aplicații din cloud. Cu Azure Active Directory Privileged Identity Management poți atribui drepturi administrative temporare, Just-In-Time (JIT), utilizatorilor eligibili pentru a gestiona resurse Azure.

Azure Role-Based Access Control (RBAC) te ajută să gestionezi accesul la resursele Azure. Acest lucru îți permite să acorzi acces în baza rolului atribuit utilizatorului, putând să furnizezi doar permisiunile de care au nevoie utilizatorii pentru a-și îndeplini sarcinile. Poți particulariza RBAC conform modelului de afaceri și toleranței față de riscuri din organizația ta.

Office 365

Soluțiile Office 365 au câteva caracteristici care te ajută să gestionezi datele cu caracter personal:

- Caracteristicile de guvernare a datelor din Centrul de securitate și conformitate Office 365 te ajută să arhivezi și să păstrezi conținut în cutii poștale Exchange Online, site-uri SharePoint Online și locații din OneDrive pentru business și să imporți date în organizația ta din Office 365.
- Caracteristica Reținere din Office 365 te poate ajuta să gestionezi ciclul de viață al e-mailului și documentelor păstrând conținutul de care ai nevoie și eliminând conținutul după ce nu mai este necesar.
- Guvernarea avansată a datelor utilizează informații și perspective asistate de computer pentru a te ajuta să găsești, să clasifici, să stabilești politici și să iei măsuri pentru a gestiona ciclul de viață al datelor care sunt cele mai importante pentru organizație.
- Politicile de gestionare a informațiilor din SharePoint Online îți permit să controlezi cât de mult este reținut conținutul, pentru a verifica ce fac persoanele cu conținutul și pentru a adăuga coduri de bare sau etichete la documente.
- Jurnalizarea din Exchange Online te poate ajuta să îndeplinești cerințe de conformitate juridică, de reglementare și organizațională prin înregistrarea comunicațiilor prin e-mail.

Clasificarea datelor

Clasificarea datelor este o parte importantă din orice plan de guvernare a datelor. Adoptarea unei scheme de clasificare care se aplică în întreaga organizație poate fi foarte utilă pentru a răspunsurile la solicitările subiecților datelor, deoarece îți permite să identifici mai prompt și să procesezi solicitările de date.

În prezent furnizăm îndrumări și instrumente pentru a vă ajuta să înțelegeți complexitatea clasificării datelor.

Azure

Materialul despre clasificarea datelor furnizează îndrumări specifice pentru clasificarea datelor în Azure și îți explică principiile din spatele tehnicilor de clasificare a datelor, procesul, terminologia și implementarea. Documentația conține o mulțime de alte informații și linkuri.

Dynamics 365

Ghidul de planificare pentru securitate și conformitate Dynamics 365 (online) furnizează îndrumări cuprinzătoare pentru înțelegerea considerațiilor cheie de conformitate și securitate asociate cu planificarea unei implementări de Dynamics 365 (online) în medii care includ servicii enterprise de integrare a directoarelor cum ar fi sincronizarea directoarelor și sign-on unic. Include informații despre confidențialitatea datelor și politicile de confidențialitate, clasificarea datelor și impact.

Enterprise Mobility + Security (EMS)

Azure Information Protection te poate ajuta să clasifici și să etichetezi datele în momentul creării sau modificării. Apoi, asupra datelor sensibile se pot aplica protecții (criptare plus autentificare plus drepturi de utilizare) sau marcaje vizuale. Etichetele de clasificare și protecțiile sunt permanente, însoțind datele pentru a putea fi identificate și protejate în permanență – indiferent unde sunt stocate sau cu cine sunt partajate.

Office și Office 365

- Prevenirea pierderii datelor (DLP) din Office și Office 365 poate identifica peste 80 de tipuri comune de date sensibile inclusiv date financiare, date medicale și informații de identificare personală. În plus, DLP permite organizațiilor să configureze măsurile care vor fi luate după identificare pentru a proteja informațiile sensibile și pentru a preveni dezvăluirea accidentală.
- Guvernarea avansată a datelor utilizează informații și perspective asistate de computer pentru a te ajuta să găsești, să clasifici, să stabilești politici și să iei măsuri pentru a gestiona ciclul de viață al datelor care sunt cele mai importante pentru organizație. Clasifică datele în baza analizei automate și recomandărilor de politici, apoi aplică acțiuni pentru menținerea datelor sau curăță ce este necesar. Datele menținute și sursele de date terțe pot fi introduse în Office 365 și clasificate după tipul de mesaj. Clasificarea tipului de mesaj permite căutarea, sortare și exportul diferitelor surse de date, ceea ce ușurează procesul de efectuare a revizuirilor ediscovery.

Windows și Windows Server

Kitul de instrumente Microsoft pentru clasificarea datelor pentru Windows Server 2012 R2 furnizează exemple de reguli și expresii de căutare pe care le poți utiliza pentru a sprijini activitățile de conformitate întreprinse de specialiștii IT, auditorii, contabilii, avocații și ceilalți specialiști din organizația ta.

Protejează: implementează controale de securitate pentru a preveni, detecta și răspunde la vulnerabilități și breșe de securitate

Organizațiile înțeleg din ce în ce mai bine importanța securității informațiilor - însă GDPR ridică standardele. Impune ca organizațiile să ia măsuri tehnice și organizaționale adecvate pentru a proteja datele cu caracter personal împotriva pierderii sau accesului ori divulgării neautorizate.

Protejarea datelor

Securitatea datelor este un domeniu complex. Există numeroase riscuri care trebuie identificate și luate în considerare - de la intruziunea fizică sau angajații rău-intenționați, până la pierderea accidentală sau atacurile hackerilor. Crearea de planuri de management al riscurilor și luarea unor măsuri de reducere a riscurilor, cum ar fi protejarea prin parolă, jurnalele de audit și criptarea, te pot ajuta să asiguri conformitatea.

Serviciul cloud Microsoft este creat special pentru a te ajuta să înțelegi riscurile și pentru a te apăra împotriva lor și este mai sigur decât mediile de calcul locale în multe privințe. De exemplu, centrele noastre de date sunt certificate la standarde recunoscute la nivel internațional, sunt protejate prin supraveghere fizică permanentă și au măsuri stricte de control al accesului.

Modul în care securizăm infrastructura cloud este doar o parte din soluția cuprinzătoare de securitate și fiecare dintre produsele noastre, în cloud sau locale, au caracteristici de securitate pentru a asigura datele.

Azure

Următoarele servicii și instrumente Azure te vor ajuta să protejezi datele cu caracter personal din mediul cloud:

- Azure Security Center îți furnizează vizibilitate și control asupra securității resurselor Azure. Acesta monitorizează continuu resursele și furnizează recomandări de securitate utile. Îți permite să definești politici pentru abonamentele Azure și grupuri de resurse în baza cerințelor de securitate ale companiei, tipurile de aplicații pe care dorești să le utilizezi și nivelul de sensibilitate a datelor. De asemenea, utilizează recomandările de securitate bazate pe politici pentru a ghida deținătorii de servicii prin procesul de implementare a mijloacelor de control necesare - de exemplu, activând programele antimalware sau criptarea discului pentru resursele tale. Security Center te ajută, de asemenea, să implementezi rapid servicii și dispozitive de securitate de la Microsoft și partenerii săi pentru a întări protecția mediului cloud.
- Criptarea datelor în Azure securizează datele în standby și în tranzit. Poți, de exemplu, să criptezi automat datele atunci când sunt scrise în spațiul de stocare Azure folosind Criptarea serviciilor de stocare. În plus, poți utiliza Azure Disk Encryption pentru a cripta sistemele de operare și discurile de date utilizate de mașinile virtuale cu Windows și Linux. Datele sunt protejate în tranzit între o aplicație și Azure astfel că rămân în permanență securizate la un nivel superior.
- Azure Key Vault îți permite să îți protejezi cheile criptografice, certificatele și parolele care te ajută să protejezi datele. Key Vault utilizează module de securitate hardware (HSM) și este conceput pentru a menține controlul cheilor și, prin urmare, al datelor, inclusiv prin asigurarea că Microsoft nu poate vedea sau extrage cheile. Poți monitoriza și audita utilizarea cheilor stocate prin intermediul capacității Azure de înregistrare și poți importa jurnalele în Azure HDInsight sau în sistemul tău de gestionare a informațiilor și evenimentelor (SIEM) pentru analiză suplimentară și detecția amenințărilor.
- Microsoft Antimalware pentru servicii cloud și mașini virtuale Azure este o capacitate gratuită în timp real care te ajută să identifici și să elimini viruși, spyware și alte programe malware care vizează furtul de date, cu alerte configurabile care te anunță atunci când programe malware sau software nedorit încearcă să se instaleze sau ruleze pe sistemele Azure.

Dynamics 365

Poți utiliza conceptele de securitate pentru Dynamics 365 pentru a proteja integritatea și confidențialitatea datelor dintr-o organizație Dynamics 365. Poți combina unități de business, securitate bazată pe roluri, securitate bazată pe înregistrări și securitatea bazată pe câmpuri pentru a defini accesul general la informațiile utilizatorilor din organizația ta Dynamics 365.

- Securitatea bazată pe roluri din Dynamics 365 îți permite să grupezi un set de privilegii care limitează activitățile care pot fi executate de un anumit utilizator. Aceasta este o capacitate importantă, în special atunci când sunt schimbate rolurile persoanelor dintr-o organizație.
- Securitatea bazată pe înregistrări din Dynamics 365 îți permite să restricționezi accesul la înregistrări specifice.
- Securitatea bazată pe câmpuri din Dynamics 365 îți permite să restricționezi accesul la anumite câmpuri de mare impact, precum cele cu informații de identificare personală.

Enterprise Mobility + Security (EMS)

În majoritatea breșelor de securitate, atacatorii obțin acces în rețeaua corporativă prin intermediul acreditărilor de utilizatori slabe, comune sau furate. Abordarea noastră față de securitate începe cu protejarea identității de la bun început cu acces condițional bazat pe riscuri.

- Azure Active Directory (Azure AD) din Enterprise Mobility + Security protejează organizația la nivel de acces prin gestionarea și protejarea identităților - și a celor privilegiate și a celor neprivilegiate. Azure AD furnizează o identitate comună protejată pentru a accesa mii de aplicații Azure AD Premium dispune de MultiFactor Authentication (MFA), care este un mijloc de control al accesului bazat pe starea dispozitivului, locația utilizatorului, identitate și riscul la conectare și pe rapoarte, audituri și alerte de securitate holistice. Azure AD Privileged Identity Management (PIM) contribuie la descoperirea, restricționarea și monitorizarea identităților privilegiate și a accesului acestora la resurse printr-un expert de securitate wizard, revizuiri și alerte. Acest lucru permite scanării precum accesul limitat în timp de tip „just in time” și „just enough administration”.

Enterprise Mobility + Security furnizează o vizibilitate asupra activității utilizatorilor, dispozitivului și datelor la nivel local și în cloud și te ajută să îți protejezi datele prin mijloace de control și aplicare solide.

- Azure Information Protection extinde controlul asupra datelor de-a lungul întregului ciclu de viață al datelor - de la creare până la stocarea locală și în servicii cloud, partajarea internă sau externă, monitorizarea distribuției fișierelor și în final răspunsul la activitățile neașteptate.
- Cloud App Security oferă vizibilitate și mijloace solide de control al datelor pentru software-ul ca serviciu (SaaS) și aplicațiile cloud pe care le utilizează angajații, pentru a avea un context complet și pentru a începe să controlezi datele cu politici detaliate.
- Microsoft Intune oferă capacități de gestionare a dispozitivelor mobile, gestionare a aplicațiilor mobile și gestionare a PC-ului din cloud. Prin intermediul Intune, poți acorda angajaților acces la aplicații, date și resurse corporative aproape de oriunde și de pe orice dispozitiv, menținând, în același timp, informațiile corporative securizate.

Office și Office 365

Platforma Office 365 include securitate la nivel de bază, de la dezvoltarea aplicațiilor până la centrele de date fizice și accesul utilizatorilor finali. Aplicațiile Office 365 includ atât caracteristici de securitate integrate care simplifică procesul de protejare a datelor, cât și flexibilitatea de a configura, gestiona și integra securitatea în moduri potrivite pentru nevoile tale de afaceri unice. Cadrul de conformitate Office 365 are peste 1.000 de mijloace de control care ne permit să menținem Office 365 la zi cu standardele din domeniu care evoluează continuu, inclusiv cu peste 50 de certificări sau atestări.

Numeroase mijloace de control sunt disponibile în mod implicit. SharePoint și OneDrive pentru business, de exemplu, utilizează ambele criptare pentru date în tranzit și în standby. În plus, poți configura și implementa certificate digitale pentru a ascunde datele cu caracter personal și poți utiliza mijloacele de control Office Access pentru a acorda și restricționa accesul la datele cu caracter personal.

Office 365 oferă alte caracteristici care te ajută să protejezi datele și să identifici când se produc breșe de securitate:

- Scorul de securitate îți oferă perspective asupra poziției de securitate și asupra caracteristicilor disponibile pentru a reduce riscurile, echilibrând, în același timp, productivitatea și securitatea.
- Advanced Threat Protection (ATP) pentru Exchange Online te ajută să protejezi în timp real e-mailul împotriva atacurilor noi, sofisticate cu malware. De asemenea, îți permite să creezi politici care te ajută să împiedici utilizatorii să acceseze atașamente sau site-uri web rău-intenționate trimise prin e-mail. ATP pentru Exchange Online include protecție împotriva programelor malware și virușilor, protecție în momentul clicului împotriva URL-urilor rău-intenționate și capacități de raportare detaliată și urmărire a URL-urilor.
- Information Rights Management (IRM) te ajută pe tine și pe utilizatorii tăi să preveniți imprimarea, redirecționarea, salvarea, editarea sau copierea informațiilor sensibile de către persoane neautorizate. Cu IRM în SharePoint Online poți limita acțiunile posibile ale utilizatorilor asupra fișierelor care au fost descărcate din liste sau biblioteci, cum ar fi imprimarea copiilor fișierelor sau copierea de text din acestea. Cu IRM în Exchange Online poți împiedica scurgerea informațiilor sensibile din mesaje e-mail și atașamente prin e-mail, online și offline.
- Management de dispozitive mobile (MDM) pentru Office 365 îți permite să configurezi politici și reguli pentru a securiza și gestiona dispozitivele iPhones, iPads, Android și telefoanele Windows înregistrate de utilizatori. De exemplu, poți șterge de la distanță un dispozitiv și poți vizualiza rapoarte detaliate pentru acesta. Office 365 utilizează, de asemenea autentificarea multi-factor pentru a furniza securitate suplimentară.

SQL Server și Bază de date SQL Azure

SQL Server și Baza de date SQL Azure oferă mijloace de control pentru gestionarea accesului la baza de date și autorizare la câteva niveluri:

- Firewallul Bazei de date SQL Azure limitează accesul la bazele de date individuale de pe serverul Bazei de date SQL Azure prin restricționarea accesului exclusiv la conexiuni autorizate. Poți crea reguli pentru firewall la nivel de server și de bază de date, specificând intervalele de IP-uri aprobate pentru conectare.
- Autentificarea la SQL Server te ajută să te asiguri că numai utilizatorii autorizați cu acreditări valide pot accesa serverul bazei de date. SQL Server acceptă atât autentificarea prin Windows, cât și datele de conectare SQL Server. Autentificarea prin Windows oferă securitate integrată și este recomandată ca opțiune mai sigură, în care procesul de autentificare este complet criptat. Baza de date SQL Azure acceptă autentificarea prin Azure Active Directory, care oferă capacitate de sign-on unic și este acceptată pentru domenii gestionate și integrate.

- Autorizarea SQL Server îți permite să gestionezi permisiunile conform principiului de acordare de privilegii minime. SQL Server și Bază de date SQL utilizează securitate bazată pe roluri, care acceptă controlul detaliat al permisiunilor pentru date prin gestionarea apartenențelor la roluri și permisiunile-la nivel de obiect.
- Mascarea dinamică a datelor (DDM) este o capacitate integrată care poate fi utilizată pentru a limita expunerea datelor sensibile prin mascarea acestora atunci când sunt accesate de utilizatori sau aplicații fără privilegii. Câmpurile de date desemnate sunt mascate rapid în rezultatele interogărilor, în timp ce datele din baza de date rămân neschimbate. DDM este ușor de configurat și nu necesită nicio modificare în aplicație. Pentru utilizatorii de Bază de date SQL Azure, mascarea dinamică a datelor poate descoperi automat datele care pot fi sensibile și pot sugera aplicarea măștilor corespunzătoare.
- Securitatea la nivel de rând (RLS) este o capacitate integrată suplimentară care permite clienților SQL Server și Bază de date SQL să implementeze restricțiile pentru accesul rândurilor de date. RLS poate fi utilizată pentru a permite accesul detaliat la rânduri dintr-un tabel de bază de date, pentru a controla mai bine ce utilizatori pot accesa datele. Având în vedere că logica pentru restricționarea accesului este localizată la nivelul bazei de date, această capacitate simplifică mult designul și implementarea securității aplicației.

SQL Server și Bază de date SQL oferă un set puternic de capacități integrate care protejează datele și identifică momentul în care se produce o breșă de securitate:

- Criptarea transparentă a datelor protejează datele în standby prin criptarea bazei de date, a copiilor de rezervă asociate și a fișierelor de înregistrare a tranzacțiilor la nivelul stocării fizice. Această criptare este transparentă pentru aplicație și utilizează accelerația hardware pentru a îmbunătăți performanțele.
- Transport Layer Security (TLS) furnizează protecția datelor în tranzit în conexiunile la Baza de date SQL.
- Always Encrypted este o caracteristică premieră în domeniu, care este concepută pentru a proteja datele foarte sensibile în SQL Server și în Baza de date SQL. Always Encrypted permite clienților să cripteze datele sensibile în interiorul aplicațiilor și să nu dezvăluie niciodată cheile de criptare către motorul bazei de date. Mecanismul este transparent pentru aplicații, deoarece criptarea și decriptarea datelor este realizată transparent într-un driver client compatibil cu Always Encrypted.

- Auditurile pentru Bază de date SQL și auditurile pentru SQL Server monitorizează evenimentele din bazele de date și le notează într-un jurnal de audit. Auditarea îți permite să înțelegi activitățile continue din baza de date și să analizezi și să investighezi activitatea istorică pentru a identifica posibile amenințări sau abuzuri și încălcări ale securității.
- Detecția amenințărilor din Bază de date SQL detectează activitățile anormale din baza de date indicând posibile amenințări asupra bazei de date. Detecția amenințărilor utilizează un set avansat de algoritmi pentru a învăța și profila în mod continuu comportamentele aplicațiilor și oferă imediat o notificare dacă detectează activități neobișnuite sau suspecte. Detecția amenințărilor te poate ajuta să îndeplinești cerințele de notificare cu privire la breșele de securitate din GDPR.

Windows și Windows Server

Windows 10 și Windows Server 2016 includ criptare lideră în domeniu, tehnologii antimalware și soluții de identitate și acces care îți permit să treceți de la parole la forme mai sigure de autentificare:

- Windows Hello este o alternativă convenabilă, de nivel enterprise, la parolele care utilizează o metodă naturală (biometrică) sau familiară (PIN) pentru validarea identității, oferind beneficiile de securitate cartelelor inteligente fără să fie necesare periferice adiționale.
- Windows Defender Antivirus este o soluție antimalware robustă care funcționează de la bun început pentru a te ajuta să te protejezi. Windows Defender Antivirus detectează rapid programele malware și poate proteja imediat dispozitivele atunci când o amenințare este observată pentru prima dată în orice parte a mediului tău.
- Device Guard îți permite să blochezi dispozitivele și serverele pentru a te proteja împotriva variantelor noi și necunoscute de malware și a amenințărilor persistente complexe. Spre deosebire de soluțiile bazate pe detecție precum programele antivirus care necesită actualizare constantă pentru a detecta cele mai noi amenințări, Device Guard blochează dispozitivele pentru a putea executa doar aplicațiile autorizate pe care le alegi, ceea ce este o modalitate eficientă de a combate programele malware.
- Credential Guard este o caracteristică ce izolează secretele pe un dispozitiv, cum ar fi tokenurile pentru sign-on unic, de acces, chiar și în cazul unei compromiteri complete a sistemului de operare Windows. Această soluție previne în principal utilizarea atacurilor greu de parat cum ar fi „pass the hash”.
- Criptare unitate BitLocker din Windows 10 și Windows Server 2016 furnizează criptare de nivel enterprise pentru a proteja datele atunci când un dispozitiv este pierdut sau furat. BitLocker criptează complet discul și unitățile flash ale computerului pentru a preveni accesul utilizatorilor neautorizați la date.

- Windows Information Protection continuă ceea ce a început BitLocker. În timp ce BitLocker protejează întregul disc al unui dispozitiv, Windows Information Protection protejează datele de utilizatorii și aplicațiile neautorizate care rulează pe un computer. De asemenea, te ajută să împiedici scurgerile de date din documente business către documente non-business sau locații locations de pe web.
- Mașinile virtuale ecranate îți permit să utilizezi BitLocker pentru a cripta discurile și mașinile virtuale (VM) care rulează pe Hyper-V, pentru a împiedica administratorii compromiși sau rău-intenționați să atace conținutul mașinilor virtuale protejate.
- Just Enough Administration și Just in Time Administration permit administratorilor să își îndeplinească sarcinile regulate, permițându-ți, în același timp, să limitezi domeniul capacităților și timpul alocate administratorilor. Dacă o acreditare privilegiată este compromisă, dimensiunea daunelor este limitată în mod semnificativ. Această tehnică furnizează administratorilor un singur nivel de acces necesar în perioada în care lucrează la proiect.

Detectarea și neutralizarea breșelor de securitate

În anumite cazuri, GDPR impune ca organizațiile să notifice rapid entitățile de reglementare, dacă se produce o breșă de securitate. În unele cazuri, organizațiile vor trebui să notifice și subiecții datelor afectate. Pentru a îndeplini această cerință, organizațiile vor beneficia de capacitatea de a monitoriza și detecta intruziunile în sistem.

Pentru incidentele în care avem responsabilitatea de a răspunde, am creat procese detaliate de Management al răspunsului la incidente de securitate așa cum s-a specificat pentru Azure și Office 365.

În plus, detaliem modul în care colaborăm cu clienții într-un Model de responsabilitate comună descris în cartea albă Responsabilități comune în Cloud Computing.

După ce detectezi breșa potențială, noi recomandăm și utilizăm pentru propriul program de răspuns la incidente un proces în patru pași:

- Evaluarea impactului și gravității evenimentului. În baza dovezilor, evaluarea poate sau nu să ducă la escaladarea către o echipă de răspuns pentru securitatea cibernetică/protecția datelor.
- Efectuezi o investigație tehnică sau legală și identifici strategiile de neutralizare, remediere și ocolire. Dacă echipa de securitate cibernetică/protecția datelor crede că datele cu caracter personal pot fi expuse unei persoane rău-intenționate sau neautorizate, un proces de notificare începe în paralel după cum o cere GDPR.

- Creezi un plan de recuperare pentru a remedia problema. Pașii de neutralizare a crizei, precum izolarea în carantină a sistemelor afectate se poate produce imediat și în paralel cu diagnosticarea. Remedierile pe termen mai lung pot fi planificate după ce riscul imediat a trecut.
- Creezi o analiză ulterioară care evidențiază detaliile incidentului, cu intenția de a revizui politicile, procedurile și procesele pentru a preveni reapariția evenimentului. Această etapă este conformă cu Articolul 31 din GDPR care impune înregistrarea faptelor din jurul breșei, a efectelor sale și a planului de remediere aplicat.

Azure

Protejarea datelor personale în sisteme, raportarea și verificarea conformității sunt cerințe cheie ale GDPR. Următoarele servicii și instrumente Azure te vor ajuta să îndeplinești aceste obligații GDPR:

- Serviciile integrate în Azure îți permit să înțelegi mai rapid și mai ușor postura de securitate generală și să detectezi și să investighezi amenințările asupra mediului tău cloud. Azure Security Center utilizează analize complexe de securitate. Sunt utilizate inovații în tehnologii big data și de învățare programată pentru a evalua evenimente în întregul sistem cloud - detectând amenințări care ar fi imposibil de identificat folosind abordările manuale și anticipând evoluția atacurilor. Aceste analize de securitate includ:
    - Investigarea integrată amenințărilor, care caută amenințările cunoscute utilizând informații globale despre amenințări de la produse și servicii Microsoft, de la Microsoft Digital Crimes Unit (DCU), de la Microsoft Security Response Center (MSRC) și din surse externe.
    - Analiza comportamentelor, care aplică modele cunoscute pentru a descoperi comportamente rău-intenționate.
    - Detecția anomaliilor, care utilizează profiluri statistice pentru a crea o line de bază istorică. Oferă alerte în cazul deviațiilor de la linii de bază cunoscute care se conformează cu un potențial vector de atac.

  În plus, Security Center furnizează alerte de securitate prioritizate care îți oferă perspective asupra campaniei de atac, inclusiv asupra evenimentelor asociate și asupra resurselor afectate.

    - Azure Log Analytics furnizează opțiuni configurabile de auditare și înregistrare de securitate care te pot ajuta să colectezi și să analizezi datele generate de resursele locale sau din cloud. Acesta oferă perspective în timp real utilizând căutare integrată și tablouri de bord particularizate pentru a analiza prompt înregistrările din toate sarcinile de lucru și serverele indiferent de locația fizică. Acesta facilitează răspunsurile rapide și investigațiile detaliate în cazul oricăror evenimente de securitate.

Dynamics 365

Întreținem și actualizăm Dynamics 365 (online) în mod regulat pentru a asigura securitatea, performanțele și disponibilitatea și pentru a oferi caracteristici și funcționalități noi. Din când în când, răspundem și la incidente de service. Pentru fiecare dintre aceste activități, administratorul Dynamics 365 pentru organizația ta primește notificări prin e-mail. În timpul unui incident de service, un reprezentant de servicii clienți Dynamics 365 (online) te poate apela telefonic și îți poate trimite ulterior un e-mail. Consultă detaliile complete ale politicilor și comunicărilor pentru Dynamics 365 pe TechNet.

Enterprise Mobility + Security (EMS)

Sistemul nostru extins de investigare a amenințărilor utilizează tehnologii de ultimă oră de analiză comportamentală și detecție a anomaliilor pentru a descoperi activitățile suspicioase și pentru a repera amenințările - atât local, cât și în cloud. Printre acestea se numără atacurile rău-intenționate cunoscute (cum ar fi Pass the Hash, Pass the Ticket) și vulnerabilitățile de securitate din sisteme. Poți lua imediat măsuri împotriva atacurilor detectate și poți simplifica recuperarea cu asistență puternică. Sistemul nostru de investigare a amenințărilor este îmbunătățit cu Microsoft Intelligent Security Graph, bazat pe un număr vast de seturi de date și pe învățare programată în cloud:

- Microsoft Advanced Threat Analytics (ATA) este un produs pentru utilizare locală, care ajută specialiștii IT să își protejeze organizația de atacuri țintite complexe prin analiza, învățarea și identificarea automată a comportamentelor normale și anormale ale entităților (utilizatori, dispozitive și resurse). ATA identifică amenințările persistente complexe (APT) la nivel local prin detectarea comportamentelor suspecte ale utilizatorilor și entităților (dispozitive și resurse), folosind învățarea programată și informațiile din Active Directory, sistemele SIEM și jurnalele de evenimente Windows de la nivel local. De asemenea, detectează atacurile rău-intenționate cunoscute (precum Pass the Hash). În final, oferă o cronologie simplă a atacurilor, cu informații clare și relevante privind atacurile, pentru a te putea concentra rapid asupra aspectelor importante.
- Cloud App Security furnizează protecție împotriva amenințărilor pentru aplicațiile tale cloud care sunt îmbunătățite cu informațiile și cercetările vaste privind amenințările din cadrul Microsoft. Poți identifica utilizarea cu risc ridicat, incidentele de securitate și poți detecta comportamentele anormale ale utilizatorilor, pentru a preveni amenințările. Euristica complexă a învățării programate din Cloud App Security analizează modul în care fiecare utilizator interacționează cu fiecare aplicație SaaS și, printr-o analiză comportamentală, evaluează riscurile din fiecare tranzacție. Sunt incluse aici autentificările simultane din două țări, descărcarea bruscă de teraocteți de date sau încercările multiple de conectare eșuate, care pot semnifica un atac în forță.

- Azure Active Directory (Azure AD) Premium furnizează detecție a amenințărilor la nivel de identitate din cloud. Azure AD monitorizează utilizarea aplicațiilor și îți protejează afacerea de amenințările complexe prin rapoarte de securitate și monitorizare. Rapoartele privind accesul și utilizarea oferă vizibilitate asupra integrității și securității directorului organizației. De asemenea, Azure AD furnizează protecția identității prin notificări, analiză și recomandări de remedii.

Office și Office 365

Office 365 are câteva capacități care te ajută să identifici brețele de securitate și să răspunzi în mod adecvat:

- Sistemul de investigare a amenințărilor te ajută să descoperi proactiv amenințările complexe și să te protejezi împotriva acestora în Office 365. Perspectivele detaliate asupra amenințărilor - disponibile în parte datorită prezenței globale a Microsoft, Intelligent Security Graph și informațiilor de la sistemele de detectare a amenințărilor cibernetice -te ajută să activezi rapid și eficient alertele, politicile dinamice și soluțiile de securitate.
- Advanced Security Management îți permite să identifici utilizarea anormală și care prezintă riscuri ridicate, alertându-te cu privire la brețele potențiale. În plus, îți permite să stabilești politici de activitate pentru a monitoriza acțiunile cu risc ridicat și activitățile suspecte și pentru a lua măsuri în cazul acestora. De asemenea, poți beneficia de Productivity App Discovery, care îți permite să utilizezi informațiile din fișierele cu jurnale ale organizației pentru a înțelege utilizarea aplicațiilor utilizatorilor din Office 365 și a altor aplicații din cloud și pentru a lua măsuri în consecință.
- Advanced Threat Protection pentru Exchange Online te ajută să protejezi în timp real e-mailul împotriva atacurilor noi, sofisticate cu malware. De asemenea, îți permite să creezi politici care te ajută să împiedici utilizatorii să acceseze atașamente sau site-uri web rău-intenționate trimise prin e-mail.

SQL Server și Bază de date SQL Azure

SQL Server și Bază de date SQL oferă un set puternic de capacități integrate care identifică momentul în care se produce o breșă de securitate:

- Auditurile pentru Bază de date SQL și auditurile pentru SQL Server monitorizează evenimentele din bazele de date și le notează într-un jurnal de audit. Auditarea îți permite să înțelegi activitățile continue din baza de date și să analizezi și să investighezi activitatea istorică pentru a identifica posibile amenințări sau abuzuri și încălcări ale securității.
- Detecția amenințărilor din Bază de date SQL detectează activitățile anormale din baza de date indicând posibile amenințări asupra bazei de date. Detecția amenințărilor utilizează un set avansat de algoritmi pentru a învăța și profila în mod continuu comportamentele aplicațiilor și oferă imediat o notificare dacă detectează activități neobișnuite sau suspecte. Detecția amenințărilor te poate ajuta să îndeplinești cerințele de notificare cu privire la breșele de securitate din GDPR.

Windows și Windows Server

Protecție avansată Windows Defender împotriva amenințărilor (ATP) permite echipelor de operațiuni de securitate să detecteze, să investigheze, să izoleze și să soluționeze breșele de securitate din rețea. Cu Windows Defender ATP, beneficiezi de capacități avansate de detecție, investigare și răspuns în caz de breșe pentru toate punctele finale cu până la 6 luni de date istorice, chiar și atunci când punctele finale sunt offline, în afara domeniului de rețea, au fost reimaginate sau nu mai există. Windows Defender ATP te ajută să îndeplinești o cerință cheie a GDPR, care are proceduri clare pentru detectarea, investigarea și raportarea breșelor de securitate.

Raportează: dă curs solicitărilor de date, raportează breșele de securitate și păstrează documentația necesară.

GDPR stabilește noi standarde de transparență, răspundere și păstrare a înregistrărilor. Va trebui să fii mai transparent nu doar cu privire la modul de gestionare a datelor personale, ci și cu privire la modul în care menții în mod activ documentația care definește procesele și utilizarea datelor cu caracter personal.

Păstrarea înregistrărilor

Organizațiile care procesează date cu caracter personal vor trebui să păstreze înregistrări cu privire la scopurile procesării, la categoriile de date cu caracter personal procesate, la identitatea terților cu care sunt împărtășite datele, la țările terțe care primesc date cu caracter personal și la baza legală a acestor transferuri, la măsurile organizaționale și de securitate tehnică și la perioadele de retenție a datelor aplicabile diferitelor seturi de date. O modalitate de a reuși acest lucru este prin utilizarea instrumentelor de auditare, care pot să asigure că orice procesare a datelor - colectare, utilizare, partajare sau de altă natură - este monitorizată și înregistrată.

Serviciile cloud Microsoft oferă servicii de auditare integrate ce te pot ajuta să te conformezi cu acest standard.

Azure, Office 365 și Dynamics 365

Pe Service Trust Portal, puteți afla informații detaliate despre diferite oferte pentru Azure, Office 365 și Dynamics 365 legate de conformitate, securitate, confidențialitate și încredere, inclusiv rapoarte și atestări. Auditurile efectuate de terți independenți și rapoartele de evaluare GRC (administrare, managementul riscurilor și conformitate) te ajută să fii la curent cu modul în care serviciile cloud Microsoft se conformează cu standardele globale care contează pentru organizația ta. Documentele cu privire la încredere te pot ajuta să înțelegi modul în care serviciile Microsoft îți protejează datele și cum poți gestiona securitatea datelor și conformitatea pentru serviciile cloud.

Azure

Auditarea și înregistrarea evenimentelor legate de securitate și a alertelor asociate reprezintă componente importante într-o strategie eficientă de protecție a datelor.

Capacitățile Azure de înregistrare și auditare îți permit:

- Să creezi un lanț de audit pentru aplicațiile implementate în Azure și pe mașinile virtuale create din Azure Virtual Machines Gallery.
- Să efectuezi analize centralizate a unor seturi mari de date prin colectarea evenimentelor de securitate din infrastructura ca serviciu (IaaS) și platforma ca serviciu (PaaS) din Azure. Poți apoi să utilizezi Azure HDInsight pentru a agrega și analiza aceste evenimente și le poți exporta în sisteme SIEM locale pentru monitorizare continuă.

- Să monitorizezi raportarea accesului și utilizării prin capacitatea Azure de înregistrare a operațiilor administrative, inclusiv accesul la sistem, pentru a crea un lanț de audit în cazul modificărilor neautorizate sau accidentale. Poți extrage jurnale de audit pentru entitatea găzduită din Azure Active Directory și poți vizualiza rapoartele privind accesul și utilizarea.
- Să exporți alerte de securitate în sisteme SIEM locale folosind Azure Diagnostics, care poate fi configurat pentru a colecta jurnale de evenimente de securitate Windows și alte jurnale de securitate specifice.
- Să obții instrumente terțe de monitorizare a securității, de raportare și alertare din Azure Marketplace.

Microsoft Azure Monitor permite organizațiilor să vizualizeze și să gestioneze cu ușurință toate activitățile de monitorizare a datelor de la un tabloul de bord central. Obții date detaliate, actualizate, privind performanțele și utilizarea, acces la jurnalul de activitate care monitorizează fiecare apelare de API și jurnale de diagnosticare ce te ajută să urmărești problemele din resursele Azure. În plus, poți configura alerte și poți lua măsuri automatizate. Azure Monitor se integrează în instrumentele existente, astfel că beneficiezi de monitorizare și analiză complete extinse prin combinarea Azure Monitor cu instrumentele de analiză cu care ești deja familiarizat.

Office și Office 365

- Asigurare servicii din Centrul de securitate și conformitate Office 365 îți oferă informații detaliate pentru a efectua evaluări ale riscurilor, cu detalii în rapoartele de conformitate Microsoft și starea transparentă a controalelor auditate, inclusiv:
- Practicile de securitate Microsoft pentru datele clienților care sunt stocate în Office 365.
- Rapoartele auditurilor efectuate de terți independenți asupra Office 365.
- Detaliile de implementare și testare pentru controalele de securitate, confidențialitate și conformitate care ajută clienții să se conformeze cu standardele, legile și reglementările din toate domeniile, cum ar fi ISO 27001 și ISO 27018, precum și Legea responsabilității și a transferabilității asigurărilor medicale (HIPAA).

- Jurnalele de audit Office 365 îți permit să monitorizezi și să urmărești activitățile utilizatorului și administratorului în sarcini de lucru din Office 365, care contribuie la detectarea și investigarea timpurie a problemelor de conformitate și securitate. Utilizează pagina de căutare a auditurilor Office 365 pentru a începe să înregistrezi activitatea utilizatorilor și administratorilor din organizația ta. După ce Office 365 pregătește jurnalul de audit, poți căuta o gamă largă de activități, inclusiv încărcările în OneDrive sau SharePoint Online ori resetările parolelor utilizatorilor. Exchange Online poate fi configurat pentru a monitoriza modificările efectuate de administratori și pentru a urmări când o cutie poștală este accesată de altă persoană decât deținătorul acesteia.
- Customer Lockbox îți conferă autoritate asupra modului în care un inginer de asistență Microsoft poate să acceseze datele în timpul unei sesiuni de asistență. În cazul în care inginerul are nevoie de acces la date pentru a depana și remedia o problemă, Customer Lockbox îți permite să să aprobi sau să respingi solicitarea de acces. Dacă o aprobi, inginerul poate să îți acceseze datele. Fiecare solicitare are un timp limită și, după rezolvarea problemei, solicitarea este închisă, iar accesul este revocat.

Enterprise Mobility + Security (EMS)

Azure Information Protection furnizează capacități extinse de înregistrare și raportare pentru a analiza modul în care datele sensibile sunt distribuite. Monitorizarea documentelor permite utilizatorilor și administratorilor să monitorizeze activitățile asupra datelor partajate și să revoce accesul în cazuri neașteptate. Azure Information Protection furnizează, de asemenea, capacități de analiză a datelor nestructurate din partajările de fișiere, site-urile și bibliotecile SharePoint, depozitele online și unitățile de desktop sau laptop. Cu accesul la fișiere poți scana conținutul fiecărui fișier și poți determina dacă în fișiere există anumite clase de date cu caracter personal. Poți, apoi, să clasifici și să etichetezi fiecare fișier în baza tipului de date prezent. În plus, poți genera rapoarte ale acestui proces, cu informații despre fișierele scanate, politicile de clasificare care s-au potrivit și eticheta care a fost aplicată.

Windows și Windows Server

Windows Event Log furnizează capacități extinse de înregistrare care permit administratorilor să vizualizeze informații înregistrate despre sistemul de operare, aplicare și activitățile utilizatorilor. Acest sistem de înregistrare poate fi configurat pentru a audita acțiuni detaliate ale utilizatorilor și aplicațiilor, inclusiv accesul la fișiere, utilizarea aplicațiilor și modificările de politică. Windows Event Log permite, de asemenea, administratorilor să redirecționeze evenimente de la clienți și servere către o locație centrală în scop de raportare și audit.

Instrumente de raportare și documentație din serviciile cloud

La fel ca în cazul oricăror alte baze de date sau sisteme care gestionează date cu caracter personal, utilizarea serviciilor cloud trebuie bine înregistrată și înțeleasă de organizația ta. De exemplu, organizația ta va trebui să înțeleagă datele cu caracter personal păstrate de furnizorii de servicii în numele organizației; relația contractuală care guvernează respectivii furnizori și ce se întâmplă cu datele atunci când o relație de servicii se încheie.

Te ajutăm să gestionezi aceste informații prin menținerea unor instrumente de raportare simple și clare cu privire la contul tău din serviciile cloud Microsoft, împreună cu documentație extinsă despre serviciile noastre cloud, modul în care funcționează și relația noastră contractuală cu tine.

Notificarea subiecților datelor

GDPR va modifica cerințele de protejare a datelor și va impune obligații mai stricte pentru procesatorii și controlorii de date cu privire la anunțarea breșelor de securitate din datele cu caracter personal care prezintă un risc pentru drepturile și libertățile individuale. În baza noii reglementări, cupă cum se definește în Articolele 17, 31 și 32, Procesatorul de date trebuie să notifice fără întârziere Controlorul de date cu privire la astfel de breșe de securitate după ce le descoperă.

După ce descoperă o breșă, Controlorul de date trebuie să notifice autoritatea relevantă de protecție a datelor în decurs de 72 de ore. Dacă breșa de securitate poate prezenta riscuri ridicate pentru drepturile și libertățile persoanelor controlorii vor trebui să notifice și persoanele afectate, fără întârziere. Aceasta însemnă că, dacă utilizezi un Procesator de date în calitate de Controlor de date trebuie să te asiguri că în contractele tale ai inclus un set clar de așteptări legate de posibilele notificări cu privire la breșe.

Pentru incidentele în care Microsoft are responsabilitatea de a răspunde, am creat procese detaliate de Management al răspunsului la incidente de securitate așa cum s-a specificat pentru Azure, Office 365 și Dynamics 365. De asemenea, menționăm angajamentele noastre față de GDPR și în contract.

Produsele și serviciile Microsoft - cum ar fi Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 și Windows 10 - au în prezent soluții disponibile pentru a te ajuta să detectezi și să evaluezi amenințările și breșele de securitate și să îndeplinești obligațiile de notificare în caz de breșe din GDPR.

Gestionarea solicitărilor subiecților datelor

Printre cele mai semnificative elemente ale GDPR se află drepturile „subiecților datelor” stipulate în Articole în Secțiunea 2: Informații și acces la date, Secțiunea 3: Rectificarea și ștergerea și Secțiunea 4: Dreptul de a obiecta și luarea automată a deciziilor în mod individual.

Aceste obligații pot avea efect asupra mediului și operațiilor IT ale Controlorului de date și asupra mediului și operațiilor IT ale oricăror furnizori de servicii angajați ca Procesatori de date.

Guvernarea adecvată a datelor a fost un element cheie al legilor privind confidențialitatea și este promovată în majoritatea legilor și regulamentelor de protecție și confidențialitate a datelor. Un element cheie al guvernării în baza GDPR este numirea unui Reprezentant de protejare a datelor (DPO) în circumstanțe specifice descrise în Articolele 35, 36 și 37. DPO trebuie să fie implicat în toate problemele legate de protecția datelor cu caracter personal.

Un al doilea element important al guvernării în baza GDPR este Revizuirea de conformitate pentru protecția datelor care generează o Evaluare a impactului asupra protecției datelor (DPIA) sub îndrumarea unui DPO. Articolul 35-*11: Dacă este necesar, controlorul va efectua o revizuire pentru a stabili dacă procesarea este executată în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când se modifică riscul reprezentat de operațiile de procesare*.

Centrul de autorizare Microsoft furnizează informații despre modurile în care putem să îți sprijinim drumul către conformitate, inclusiv o secțiune specială despre viziunea și angajamentele Microsoft față de GDPR.