Conformarea la GDPR în IT: Angajaţii

Deşi implementarea şi respectarea regulamentului GDPR cade, de obicei, în grija unei persoane desemnate sau a unei echipe, toţi angajaţii din companie vor trebui să fie puşi la curent cu noile norme. Când vine vorba de GDPR în IT, miza este destul de mare, având în vedere cantitatea considerabilă de date preluate şi prelucrate în mod constant.

Chiar şi o mică neglijenţă sau neatenţie poate avea consecinţe deosebit de grave cu privire la nivelul de securitate al datelor sensibile. Deoarece persoanele desemnate să aibă grijă de implementarea regulamentului ştiu ce au de făcut, breşa de securitate poate exista în rândul angajaţilor. Iată ce trebuie făcut pentru a te asigura că nu vor exista probleme.

Toţi angajaţii trebuie să fie informaţi cu privire la noile norme de securitate

Atâta timp cât o persoană activează în cadrul companiei dumneavoastră, trebuie să fie mai mult decât conştientă de existenţa noilor norme de securitate în ceea ce priveşte datele cu caracter personal. Puteţi opta pentru servicii GDPR în acest sens, aducând în cadrul companiei persoane care vor informa corect toţi angajaţii dumneavoastră. GDPR Advisors este o companie de consultanţă GDPR care oferă acest tip de servicii, aşadar nu ezitaţi să solicitaţi ajutor adecvat. Atunci când informarea este făcută de persoanele potrivite, procesul este mai scurt şi eficient, astfel încât toată lumea îşi reia activitatea cât mai curând cu putinţă.

Ce trebuie un angajat să ştie?

Orice angajat trebuie să cunoască modalitatea corectă de

autentificare şi delogare în şi din sistemele folosite de companie. O operaţiune de acest gen efectuată greşit sau ignorată poate crea breşe de securitate.

Dacă se utilizează aplicaţii, angajaţii trebuie să ştie cum şi când acestea se folosesc. Trebuie determinate aplicaţiile pentru care este permisă operarea de date cu caracter personal, iar lista va trebui înmânată fiecărui angajat.

Dacă utilizaţi filtre pentru traficul realizat pe Internet sau ce privesc folosirea e-mail-ului, aveţi grijă să spuneţi angajaţilor că acest lucru se întâmplă şi scopul pentru care aceste filtre sunt folosite. Filtrarea este recomandată pentru că sporeşte securitatea, nepermiţând clonarea website-urilor pentru a putea obţine informaţii din interiorul lor.

Este recomandat să monitorizaţi şi modul în care calculatoarele din cadrul companiei sunt folosite, astfel încât să puteţi găsi erorile atunci când ele se întâmplă. Dar, acest lucru este unul ce trebuie adus şi la cunoştinţa angajaţilor. Ei trebuie să ştie că echipamentele pe care le folosesc sunt monitorizate, din motive de securitate şi respectare a GDPR-ului.

Dacă supravegheaţi birourile cu camere web sau aveţi access la conversaţiile, atât telefonice cât şi pe chat, între angajaţi, asiguraţi-vă că toată lumea ştie despre aceste lucruri. Compania dumneavoastră poate face astfel de monitorizări atunci când vine vorba de sporirea securităţii şi calitatea proceselor din cadrul companiei. Aşadar, angajaţii trebuie să înţeleagă că nu e vorba de spionaj sau monitorizare a persoanelor, ci doar măsuri sporite de protecţie care vor ajuta la găsirea sursei problemelor, dacă şi când acestea vor avea loc.

În cazul în care angajaţii dumneavoastră primesc dispozitive mobile şi au voie să le folosească în afara companiei, aduceţi-le la cunoştinţă modalitatea în care le pot folosi. De

asemenea, ar fi ideal să criptaţi astfel de dispozitive, atfel încât să nu existe scurgeri accidentale de date.

Învăţaţi angajaţii să folosească parole adecvate şi ce înseamnă o parolă de încredere. Instruiţi-i şi cu privire la utilizarea memoriilor de tip flash, a USB-urilor, şi a conexiunilor Bluetooth. Dacă există o politică de backup în cadrul companiei, şi angajaţii trebuie să ştie despre ea şi cum se face un backup de date corect.

Alte recomandări

O autentificare bazată pe doi factori, în loc de unul singur, este mai sigură, în cazul în care parola setată ajunge să fie compromisă.

Ar trebui puse la punct procedure special pentru cazurile în care compania angajează sau se desparte de un angajat, pentru că şi aici vorbim de managementul datelor cu caracter personal, iar GDPR-ul trebuie respectat şi în cazul persoanelor ce lucrează într-o companie, nu doar pentru persoanele din exteriorul instituţiei.

Nu este deloc recomandat ca mai mulţi utilizatori să folosească acelaşi tip de user şi parolă pentru a se loga la un sistem. În cazul în care o problem va apărea, va fi greu să determinaţi cine este responsabil. Pe lângă acest aspect, folosirea aceluiaşi user şi aceleaşi parole pentru toata lumea va face sistemul vulnerabil.

Concluzie

Menţineţi o evidenţă clară a tipurilor de acces pe care le permiteţi în companie, cu cine şi la ce tip de informaţie sau sistem are acces. De asemenea, setaţi limitări şi nu oferiţi cheile de acces decât persoanelorautorizate.

Sursa: GDPR Advisors