

Conformarea la GDPR în IT: Angajații

Deși implementarea și respectarea regulamentului GDPR cade, de obicei, în grija unei persoane desemnate sau a unei echipe, toți angajații din companie vor trebui să fie puși 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 și prelucrate în mod constant.

Chiar și o mică neglijență sau neatenție poate avea consecințe deosebit de grave cu privire la nivelul de securitate al datelor sensibile. Deoarece persoanele desemnate să aibă grijă de implementarea regulamentului știu ce au de făcut, breșa de securitate poate exista în rândul angajaților. Iată ce trebuie făcut pentru a te asigura că nu vor exista probleme.

Toți angajații trebuie să fie informați cu privire la noile norme de securitate

Atâta timp cât o persoană activează în cadrul companiei dumneavoastră, trebuie să fie mai mult decât conștientă de existența noilor norme de securitate în ceea ce privește datele cu caracter personal. Puteți opta pentru servicii GDPR în acest sens, aducând în cadrul companiei persoane care vor informa corect toți angajații dumneavoastră. [GDPR Advisors](#) este o companie de consultanță GDPR care oferă acest tip de servicii, așadar nu ezitați să solicitați ajutor adecvat. Atunci când informarea este făcută de persoanele potrivite, procesul este mai scurt și eficient, astfel încât toată lumea își reia activitatea cât mai curând cu putință.

Ce trebuie un angajat să știe?

Orice angajat trebuie să cunoască modalitatea corectă de

autentificare și delogare în și din sistemele folosite de companie. O operațiune de acest gen efectuată greșit sau ignorată poate crea breșe de securitate.

Dacă se utilizează aplicații, angajații trebuie să știe cum și când acestea se folosesc. Trebuie determinate aplicațiile pentru care este permisă operarea de date cu caracter personal, iar lista va trebui înmănată fiecărui angajat.

Dacă utilizați filtre pentru traficul realizat pe Internet sau ce privesc folosirea e-mail-ului, aveți grijă să spuneți angajaților că acest lucru se întâmplă și scopul pentru care aceste filtre sunt folosite. Filtarea este recomandată pentru că sporește securitatea, nepermițând clonarea website-urilor pentru a putea obține informații din interiorul lor.

Este recomandat să monitorizați și modul în care calculatoarele din cadrul companiei sunt folosite, astfel încât să puteți găsi erorile atunci când ele se întâmplă. Dar, acest lucru este unul ce trebuie adus și la cunoștința angajaților. Ei trebuie să știe că echipamentele pe care le folosesc sunt monitorizate, din motive de securitate și respectare a GDPR-ului.

Dacă supravegheați birourile cu camere web sau aveți access la conversațiile, atât telefonice cât și pe chat, între angajați, asigurați-vă că toată lumea știe despre aceste lucruri. Compania dumneavoastră poate face astfel de monitorizări atunci când vine vorba de sporirea securității și calitatea proceselor din cadrul companiei. Așadar, angajații trebuie să înțeleagă că nu e vorba de spionaj sau monitorizare a persoanelor, ci doar măsuri sporite de protecție care vor ajuta la găsirea sursei problemelor, dacă și când acestea vor avea loc.

În cazul în care angajații dumneavoastră primesc dispozitive mobile și au voie să le folosească în afara companiei, aduceți-le la cunoștință modalitatea în care le pot folosi. De

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

Învățați angajații să folosească parole adecvate și ce înseamnă o parolă de încredere. Instruiți-i și cu privire la utilizarea memoriilor de tip flash, a USB-urilor, și a conexiunilor Bluetooth. Dacă există o politică de backup în cadrul companiei, și angajații trebuie să știe despre ea și 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 și aici vorbim de managementul datelor cu caracter personal, iar GDPR-ul trebuie respectat și în cazul persoanelor ce lucrează într-o companie, nu doar pentru persoanele din exteriorul instituției.

Nu este deloc recomandat ca mai mulți utilizatori să folosească același tip de user și parolă pentru a se loga la un sistem. În cazul în care o problemă va apărea, va fi greu să determinați cine este responsabil. Pe lângă acest aspect, folosirea aceluiași user și aceleași parole pentru toată lumea va face sistemul vulnerabil.

Concluzie

Mențineți o evidență clară a tipurilor de acces pe care le permiteți în companie, cu cine și la ce tip de informație sau sistem are acces. De asemenea, setați limitări și nu oferiți cheile de acces decât persoanelor autorizate.

Sursa: [GDPR Advisors](#)