Gederd teab, kuidas mitte eksida

Isikuandmete kaitse üldmäärusega (GDPR)

Lahenduste teejuht

squalio

Sissejuhatus

Gederdi lahenduste teejuht on kasulik kokkuvõte nõuetest, mida alates 2018.a. 25.maist hakatakse Isikuandmete kaitse üldmääruse alusel (GDPR) kohaldama isikuandmete kaitsele Euroopa Liidus, ning olulistest toimingutest, mida ettevõte peab teostama, et need nõuded oleksid järgitud töös isikuandmetega.

GDPR puudutab kõiki ettevõtteid, mis töötavad isikuandmetega EL's, mis müüvad tooteid või osutavad teenuseid EL'i elanikele, ning mis teostavad järelevalvet EL'i elanike toimingute üle. Kavandatud muudatused on laiad ning mõjutavad paljusid ettevõtte funktsioone.

Teejuht

GDPR NÕUDED	VIIDE GDPR'le	TÄPSEM TEAVE	IGAPÄEVA NÄITED, KUS KERKIB ESILE GDPR KOHALDAMINE	ETTEVÕTTE POOLT TEOSTATAVAD TOIMINGUD	SOOVITATUD IT LAHENDUSED
Andmete töötlemise seaduslikkus	§6, §7 ja §8	Isiku andmeid saab kasutada: 1. kui isik on andnud selleks oma nõusoleku; 2. kui see on vajalik kooskõlas seadusega. Füüsiline isik (andmete omanik) on õigustatud võtma oma nõusolek tagasi.	1. Isikuandmeid on võimalik saada neid kirjutades üles, e-posti teel või kopeerides isiku passi, sest nii on mugavam teostada või hallata kandeid vastava isiku kohta. 2. Võimalik, et soovite, et isik esitaks oma isikutunnistuse või passi koopia, arvates, et see garanteerib isiku tuvastamise, kuid sellist võtet seadus ei nõua ega luba.	1. Tuleb teadvustada ja defineerida ettevõtte põhjendus andmete saamiseks ja töötlemiseks. 2. Tuleb saavutada isiku nõusolek andmete saamiseks ja kasutamiseks. 3. Tuleb tagada andmete kustutamine, kui andmete omanik seda nõuab.	1. Office 365 E3 võimaldab kogu ettevõtte teavet ja andmeid hoida ühes kohas. See on üks olulisematest IT turvalisuse põhinõuetest, et ettevõte saaks kontrollida teabe ja andmete vahetamist ettevõtte siseselt. (SharePoint Online)
Andmete klassifi-tseerimine	§9, §10 ja §11	Ettevõte peab teadma, millist liiki andmeid see hoiab. Andmeid saab jagada järgnevatesse kategooriatesse: 1. Kõrgeima astme kategooriad: avalikud või konfidentsiaalsed andmed; 2. Alakategooriad: ärisaladus, andmed sisemiseks kasutamiseks, personali juhtimisega seotud teave, finantsandmed, IT andmed jm; 3. Erikategooria: tundlikud andmed.	1. On oluline pidada meeles, et seadus piirab andmete hankimist selle kohta, kas isik ootab last, kas ta on mõne ametiühingu või poliitilise partei liige. 2. Praktikas on sageli nii, et ettevõttes ei ole ühist arusaama selle kohta, milline teave on konfidentsiaalne ja milline mitte, töötajad ei saa aru, millal ja millistel juhtudel nad riskivad, kui töötlevad andmeid. Sellepärast tuleb ettevõttes defineerida, millist liiki teavet tuleb eriti kaitsta.	1. Tuleb luua isikuandmete võtmesõnu, mille järgi on võimalik selliseid andmeid korrastada ja leida - ees-, perekonnanimi, ID number (nt isikukood), aadress, tänav, maja, number ja linn. 2. Tuleb veenduda, et andmed oleksid hoiul piiratud ligipääsuga kohas, nimelt ligipääs andmetele on vaid teatud isikutele. Andmeid tuleb korrastada võtmesõnade järgi (nt passide pdf koopiad, välised serverid).	1. Office 365 E3 hõlmab detailset andmete otsimist, mis kiiresti leiab vajalikud andmed mistahes ettevõtte inforessursist. (eDiscovery) 2. Office 365 E3 markeerimisfunktsioon pakub võimalust jagada andmeid automaatselt kategooriateks võtmesõnade järgi, jättes võimalust muuta kategooriaid käsitsi.

GDPR KÜSIMUSED	VIIDE GDPR'le	TÄPSEM TEAVE	IGAPÄEVA NÄITED, KUS KERKIB ESILE GDPR KOHALDAMINE	ETTEVÕTTE POOLT TEOSTATAVAD TOIMINGUD	SOOVITATUD IT LAHENDUSED
Juurdepääsu õigus andmetele	§12, §13, §14, §15, §16, §17, §18, §20, §21 ja §22 §24, §27, §28.	Juurdepääsu õigust andmetele tuleb tagada vaid juhul, kui see on kindlale isikule tõesti vajalik tööülesannete täitmiseks.	1. Võimaldades kõikidele töötajatele juurdepääsu kõikidele andmetele, ettevõte riskib sellega, et mõni töötaja saab lekitada isikuandmeid või ettevõttele olulist teavet mistahes mahus. 2. Kui töötaja tekitab ettevõttele kahju teabe või isikuandmete lekitamisega, siis lahendus, mis võimaldab andmetele juurdepääsu piiramist, aitab tuvastada isiku, kes on pääsenud ligi teabele ja seda lekitanud, ning nõuda kahju hüvitamist vastava töötaja käest. See võib olla ka põhjuseks töölt vabastamiseks.	1. Töötajatele tuleb tagada ettevõtte andmetele individuaalsed juurdepääsu õigused. 2. Igale töötajale tuleb tagada identifikaator – kood, millega töötaja identifitseeritakse IT süsteemis. 3. Igale töötajale peab olema tagatud unikaalne, turvaline parool juurdepääsuks andmetele.	1. Office365 E3 moodustab individuaalseid töötajate identifikaatoreid ja töötajate rühmasid võimalusega määrata individuaalset juurdepääsu kindlatele kaustadele või andmetele. 2. Lahendus pakub ka madalamaid juurdepääsu õiguseid eraldi posti ja dokumentide kaustadele. 3. Office365 E3 määrab paroolide loomisel turvalisuse kriteeriume, mille järgimata jätmise korral, töötaja parooli ei saa luua. (O365 Active Directory)
Kasutuses olevad ressursid	§24, §26, §28.	Ettevõttes kasutusel olevate andmete hoiustamise ja muude IT ressursside identifitseerimine aitab määrata vajalikke ohutusmeetmeid igale ressursile eraldi. Need on: 1. serverid, programmid; 2. e-post; 3. internetiühendus; 4. mobiili ja kaasaskantavad seadmed; 6. võrguketad või kaustad; 7. töötaja isiklikud arvutid või muud seadmed.	1. Mõnikord ettevõtted unustavad serverid või muud kasutusel olevad andmete hoiustamise kohad. Olenemata sellest, kus teavet hoitakse, on kogu selline informatsioon kaitse all. 2. Kui töötajad kasutavad ettevõtte tarbeks oma era e-posti, siis ei ole võimalik tagada andmevoo kaitset ja andmetele juurdepääsu kontrollimist. 3. Ebaturvalise või ebapiisava turvalisusega pilveteenuse või paroolita seadme kasutamine tekitab tõsist andmete turvalisuse riski.	1. Tuleb vähendada kasutatavate ressursside erinevust. 2. Tuleb kasutada vaid turvalisi ja sertifitseerituid andmete hoiustamise ja tööks vajalikke ressursse ja lahendusi, et tagada vastavat andmekaitse taset.	1. Office 365 E3 hoiustab andmeid pilves, mis on sertifitseeritud vastavalt GDPR nõuetele. 2. Lahendus näeb ka ette eraldi andmekaitset juhul, kui töötajad töötavad isiklike seadmetega, võimaldades pääseda ettevõtte andmetele ligi vaid turvaliste seadmete kaudu. (Mobile Device Manager) 1. Andmete otsimine ja andmetega seotud toimingute auditeerimine on kättesaadav kogu Office 365 E3 ulatuses.

GDPR KÜSIMUSED	VIIDE GDPR'le	TÄPSEM TEAVE	IGAPÄEVA NÄITED, KUS KERKIB ESILE GDPR KOHALDAMINE	ETTEVÕTTE POOLT TEOSTATAVAD TOIMINGUD	SOOVITATUD IT LAHENDUSED
Andmete hoiustamine	§ 30	Isikuandmeid tuleb hoiustada ettevõtte siseprotseduuride kohaselt ja kooskõlas kohaldatavate seadusnõuetega.	1. Igal andmeühikul on ettenähtud hoiustamise periood, mille määravad kohaldatavad seadused või ettevõtte sisereeglid. Selline andmete hoiustamise nõuete mittejärgmine võib olla aluseks sanktsioonide kohaldamisele vastutavate riigiasutuste poolt või muud liiki vastutuse tekkimisele. 2. Õige andmete hoiustamine tagab selle, et ettevõte suudab esitada dokumentaalseid tõendeid oma tegevuse või tegevusetuse kohta, kui see on vajalik nt vaidluses andmete omanikuga või kohtumenetluses. See on oluline, sest kohtusse saab pöörduda kogu nõudeõiguse kehtivusaja jooksul, mis võib olla isegi kuni 10 aastat pikk.	1. Tuleb tagada tehniline võimalus säilitada andmeid kindla aja jooksul. 2. Tuleb tagada võimalus sorteerida andmeid kategooriatesse või vastavalt hoiustamise tähtajale. 3. Tuleb tagada võimalus jälgida seda, millal lõpeb andmete hoiustamise tähtaeg ja millal tuleb andmed kustutada või hävitada.	1. Office365 E3 tagab andmete hoiustamise, mis põhineb andmete markeeringutel ja tundliku teabe tüüpidel. 2. Lahendus tagab automaatse hoiustatud andmete kustutamise vastavalt ettevõtte või seaduses ettenähtud andmete hoiustamise poliitikale.
Andmete järelevalve	§24, §26, §28, §30.	Kõik isikuandmetega seotud toimingud tuleb dateerida, hoiustada ja järelevalvata.	1. Kui töötaja tekitab ettevõttele kahju teabe lekitamisega, siis on oluline tuvastada isik, kes on pääsenud teabele ligi ja seda lekitanud, ning nõuda kahju hüvitamist vastava töötaja käest. See võib olla ka põhjenduseks töölt vabastamiseks. 2. Sisseauditeerimine võib aidata avastada ettevõtte IT turvalisuse nõrgemaid punkte ning saada ülevaadet sellest, millistele ettevõtte süsteemidele pääsetakse ligi kõige sagedamini ja kes seda teeb.	1. Tuleb määrata vastutav töötaja, kes teostab isikuandmetega seotud töö ja tegevuste järelevalvet. 2. Peab olema tagatud võimalus leida üles hoiustatud andmed konkreetse isiku kohta. 3. Peab olema tagatud võimalus säilitada viimaseid toiminguid ja sissekandeid. 4. Tuleb regulaarselt viia läbi sise- või välisaudit.	1. Office 365 tagab võimalust leida sissekandeid konkreetsete isikuandmetega teostatud toimingute kohta. (eDiscovery, Audit Logs) 2. Lahendus annab ülevaate viimastest toimingutest, mis on teostatud isikuandmetega. (Document History, Audit Logs)

GDPR NÕUDED	VIIDE GDPR'le	TÄPSEM TEAVE	IGAPÄEVA NÄITED, KUS KERKIB ESILE GDPR KOHALDAMINE	ETTEVÕTTE POOLT TEOSTATAVAD TOIMINGUD	SOOVITATUD IT LAHENDUSED
IT turvalisus	§32, §33, §34.	Juurdepääs ettevõtte andmetele ja andmetöötlusele peab toimuma vastavalt IT turvanõuetele.	1. Kui ettevõte ei võta kasutusele mingeid ohutuslahendusi, siis töötajad ei pööra andmete turvalisusele piisavalt suurt tähelepanu. Endiselt esineb komme edastada tundlikke andmeid e-posti teel teistele töötajatele, koostööpartneritele või klientidele. Kui mõne töötaja tõttu tekib isikuandmete leke, siis ettevõttel on kohustus sellisest lekkest teavitada riigiasutusi, mis vastutavad andmekaitse eest, ning ka puudutatud isikuid tuleb informeerida nende isikuandmete lekke fakti kohta. Sellesel juhul nii ettevõte kui ka leket põhjustanud töötaja peab võtma seaduses ettenähtud vastutuse. 2. Andmete tagavarakoopiate loomine tagab seaduses ettenähtud andmete hoiustamise nõuete järgimise.	1. (Sisemistest/väimistest) turvalisuse rikkumistest peab ettevõtte vastutav isik teavitama riigi asutusi ja andmete omanikku. 2. Tuleb taastada andmete turvalisus ja võtta kasutusele tehnilised lahendused. Ettevõte peab veenduma andmete turvalisuses ka manuaalselt. 3. Tuleb tagada andmete tagavarakoopiad.	1. Office365 E3 tagab automatiseeritud häireteated, kui on toimunud autoriseerimata juurdepääs andmetele või nende leke. (Alerts) 2. Turvalisuse taastamist intsidendi korral tagab Office365 turvatugi, millega saab võtta ühendust ööpäevaringselt (24/7). 3. Lahendus tagab automaatse tagavarakoopia loomise ning võimaldab täielikku andmete taastamist, kui on toimunud rünnak andmetele.

squalio

Tööta andmetega turvaliselt

www.gederd.ee

squalio