

SAVLAICĪGA GDPR PRASĪBU ĪSTENOŠANA

WatchGuard®

Saturs

Sacensība līdzi laikam! 3

Kas ir iesaistīti šajās sacensībās? 4

Ko var uzskatīt par personīgo informāciju? 5

Uzmanīšanās no apdraudējumiem. 6

- Personas datu aizsardības pārkāpumu paziņojumi 6
- Nepārprotama piekrišana 6
- Datu pārsūtīšana ārpus ES 6
- Datu aizsardzības pārziņa norīkošana 7
- Sodi un izmaksas par neatbilstību 7

Uzvaras stratēģija 8

GDPR prasību izpilde 9

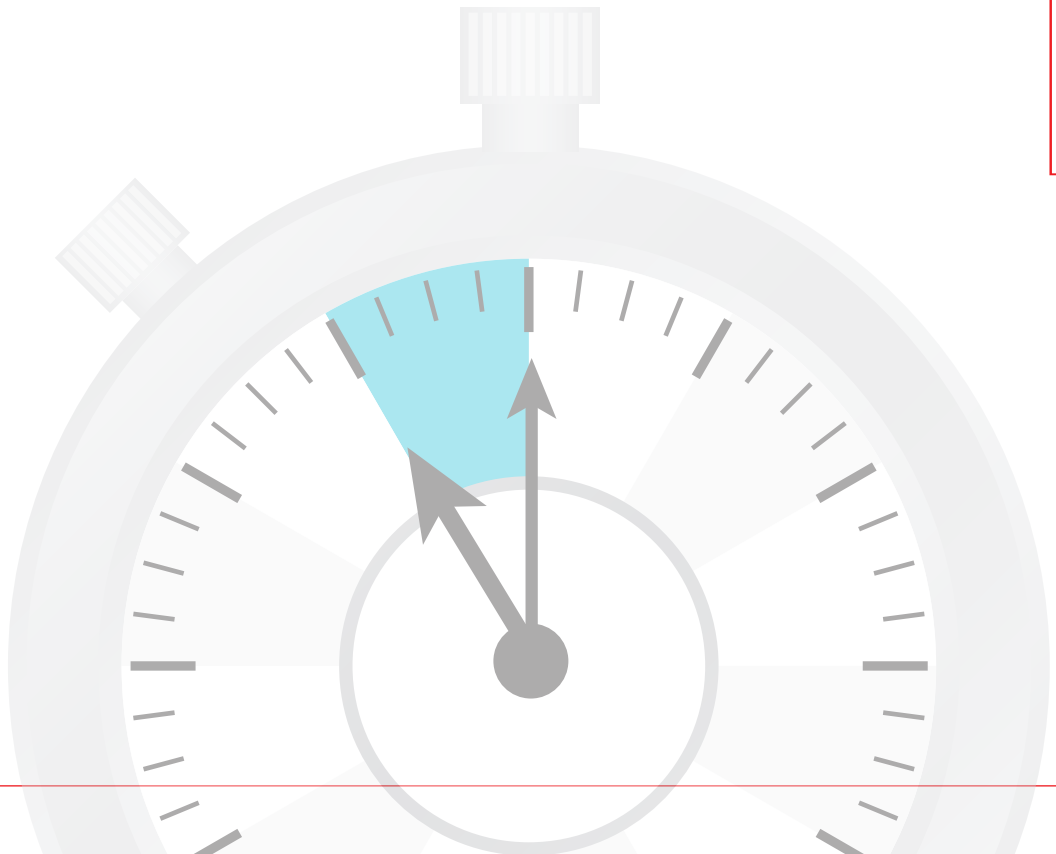
GDPR veicamo darbu saraksts 14

Sacensība līdzi laikam!

Sākot ar 2016. gada aprīli, pielāgojoties Vispārīgajai datu aizsardzības regulai (General Data Protection Regulation (GDPR), (EU) 2016/679), kompānijas steidz to īstenot, lai sasniegtu atbilstību šai regulai pirms tā stājas spēkā 2018. gada 25. maijā, un nesaskartos ar sodiem un juridiskajām sankcijām. Salīdzinot ar līdz šim spēkā esošo Datu aizsardzības direktīvu (Directive 95/46/EC), kura ir spēkā kopš 1995. gada, šī aptvers daudz plašākas atbildības jomas un prasīs krietni vairāk pūļu, lai to varētu ieviest, un ievērot noteiktās prasības.

Labā ziņa – **tu neesi vienīgais!** Tas ir kā sacensībās - visi sāk no vienādām pozīcijām, un tikai sadarbojoties mēs sasniegsim gala rezulātu ātrāk un vieglāk.

Šajā materiālā tiek piedāvāta svarīgākā informācija par Visparīgo datu aizsardzības regulu (GDPR) un piedāvā risinājumus atbilstoši šai iniciatīvai, lai uzlabotu jūsu datu drošību.



Vispārīgā datu aizsardzības regula stājas spēkā sākot ar **2018. gada 25. maiju**



Kas ir iesaistīti šajās sacensībās?

Organizācijām, kas vāc, glabā un/vai apstrādā personu datus, ir nepieciešams pilnībā atbilst Vispārīgās datu aizsardzības regulas prasībām, ja:

- piedāvā un sniedz pakalpojumus Eiropas savienībā

  VAI

- uzrauga Eiropas savienības pilsoņus Eiropas savienības teritorijā

Tas skars arī organizācijas, kuras nav bāzētas Eiropas savienībā, un protams arī tās orgaizācijas, kur strādā Eiropas savienības pilsoņi. Tātad, ja Jūs glabājat kāda veida personīgo informāciju, kas saistīta ar Eiropas savienības pilsoņiem... Tas attiecas arī uz Jums!

Visām organizcijām, kuras atbilst šiem kritērijiem, šī regula būs jāievēro. Tomēr, organizācijām, kurās būs nodarbināti vairāk par 5,000 darbiniekiem, būs vēl paplašinātas prasības.

Piemēram, veselības aprūpes iestādes var uzticēt laboratorijas darbus citai iestādei. Klīnikai būtu jādalās ar personīgo informāciju, kura ievākta laboratorijas vajadzībām, lai rezultāti nonāktu pie pareizajiem pacientiem. Šajā situācijā veselības aprūpes iestāde ir kontrolieris, un laboratorija ir procesors, atbilstoši Vispārīgās datu aizsardzības regulas formulējumam. Šeit ir dažas atšķirības regulas prasībās katrai no pusēm, un jums jānosaka, kurai no pusēmJūs piederat, vai varbūt pat abām.

Ko var uzskatīt par personīgo informāciju?

Vispārīgā datu aizsardzības regula personas datus definē ļoti plaši. Jebkāda daļa informācijas, kas tiešā vai netiešā veidā identificē personu, ir uzskatāma par personīgajiem datiem. Tas var būt kaut vai vārds, foto, e-pasta adrese, bankas rekvizīti, ID kartes numurs, ieraksti no sociālajiem tīkliem, medicīnikā informācija, un arī datora IP adrese, kas attiecas uz kādu lietotāju vai ierīci.

Piemēram, ir nepieciešams strādāt ar sacensību dalībnieku numuriem, kur dalībnieka numurs atbilst kādai personai, un ievadīt tos sistēmā, tad tie arī ir uzskatāmi par personas datiem. Turklāt šie skaitļi bieži vien sasaucas ar foto, iepējams pat ar medicīnas datiem un pat adresi.





The peloton
Photo: Sue Hixson

Uzmanīšanās no apdraudējumiem

Vispārīgā datu aizsardzības regula ietver daudzas lietas, kas agrāk nebija Datu aizsardzības direktīvā, un var skart arī Jūs pat, tad ja vecā direktīva Jūs neskāra. Lūk arī dažas no visievērojamākajām prasībām.

- **PERSONAS DATU AIZSARDZĪBAS PĀRKĀPUMU PAZIŅOJUMI:** tagad būs nepieciešams 72 stundu laikā kopš datu noplūdes brīža paziņot uzraudzības iestādēm, un paziņot arī personām, kuru personas dati ir kompromitēti.

Svarīgi, ka **šifrētu datu** uzlaušana ir **īpašs izņēmums,** jo paziņošanai vajadzētu notikt atbilstoši stratēģijai.

- **NEPĀRPROTAMA PIEKRIŠANA**: GDPR paredz, ka brīdī, kad Jūs savācat personas datus, ir jābūt nepārprotamai piekrišanai no personas, kuras dati tiek ievākti. Tas nozīmē, ka organizācijas vairs nevarēs prasīt vien vispārīgu piekrišanu. Tā vietā, organizācijām jāpiedāvā konkrētu informāciju par to kādi dati tiks apkopoti, kā dati tiks uzglabāti un apstrādāti, un jālieto skaidra un vienkārša valoda.

- **DATU PĀRSŪTĪŠANA ĀRPUS ES:** Personas datus nedrīkst izvest ārpus ES, ja vien Jums nav apstiprinājums no uzraudzības iestādēm vai, ja datu subjekts ir informēts par datu tālāku nodošanu un ar to saistītajiem riskiem, un datu subjekts atļauj to nodošanu.

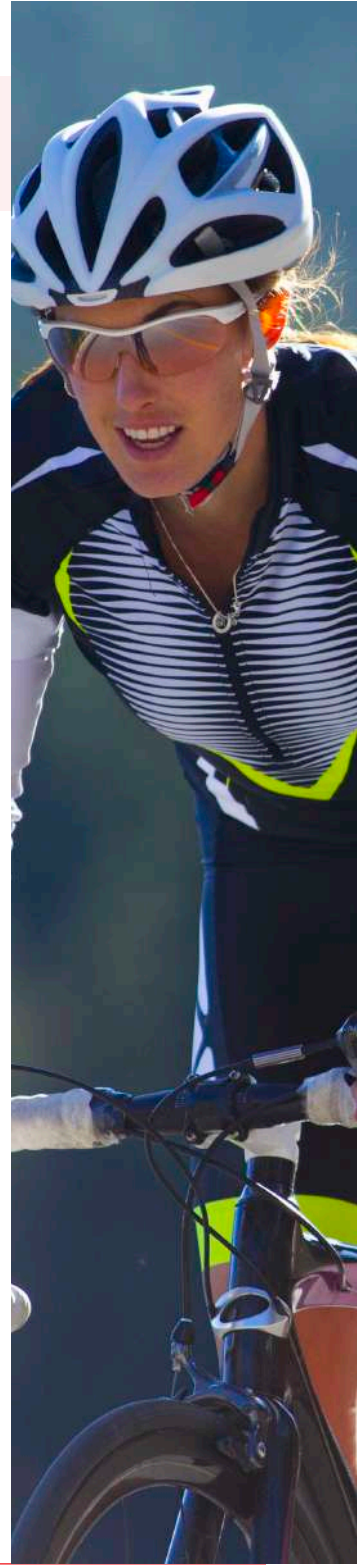


- **DATU AIZSARDZĪBAS PĀRZIŅA NORĪKOŠANA:** Ja Jūs apstrādājat datus par vairāk nekā 5000 personām, jebkurā 12 mēnešu periodā, tad Jums ir jāieceļ/jānorīko Datu aizsardzības pārzinis (DPO) Jūsu organizācijai. DAP ir Jūsu pārstāvis sadarbojoties ar uzraudzības iestādēm, kas seko un nodrošina atbilstību regulai. Viņš vai viņa ir arī kontaktpersona jebkādām prasībām vai sūdzībām no datu subjektiem. Bez tam, viņu pienākumos ir arī, piemēram, Datu aizsardzības ietekmes novērtējuma (DPIA) izveide, un rīkoties saskaņā ar drošības politiku, apstrādāt un pieņemt pieprasījumus no datu subjektiem, un paziņojumus par pārkāpumiem.

Organizācijām var piespriest sodu līdz pat €20 miljoniem vai 4% no kopējā uzņēmuma apgrozījuma

- **SODI UN IZMAKSAS PAR NEATBILSTĪBU:** Uzņēmumi un organizācijas, kuras neievēros šo regulu, var tikt sodītas līdz pat €20 miljonu apmērā, vai arī 4% no kopējā uzņēmuma apgrozījuma. Sodi tiek iedaliti un izvertēti pat pēc pirmreizējiem pārkāpumiem, un soda nauda par nepareizi sakārtotiem dokumentiem var būt pat līdz 2% no uzņēmuma ienākumiem (atsaucoties uz 28. pantu). Uzņēmumiem var nākties segt arī juridiskos un tiesas izdevumus, ja cietušais uzskata, ka viņa tiesības ir aizskartas un ir radīti zaudējumi.





Uzvaras stratēģija

Gandrīz visiem uzņēmumiem tas prasīs lielu piepūli, lai atbilstu regulas prasībām un tas ietver:

- Datu aizsardzības pasākumus, **izmantojot jaunākās, visefektīvākās tīkla aizsardzības tehnoloģijas** kuras:
  - **aizsargā datus** gan tos uzglabājot, gan tos pārsūtot
  - nodrošina **situācijas izpratni** saistībā ar riskiem
  - ļauj iespēju veikt **preventīvos pasākumus un ietekmi mazinošus pasākumus reālā laikā** pret ievainojamībām un apdraudējumiem
  - nodrošina **rīkus, lai novērtētu** drošības politiku efektivitāti
- Datu atgūšanas mehānismi, kuri atjauno piekļuvi datiem, kad incidents traucē pieejamību tiem
- Jaunas un uzlabotas procedūras paziņošanai par pārkāpumiem, par atbilstību prasībām un par piekrišanu izsekošanai

Jums vajadzētu arī apsvērt iespējas samazināt riskus balstoties uz regulā noteiktajām prasībām, kas ir saistītas ar uzraudzību, uzskaiti un darbību atbilstību.

Piemēram:

- **Samazināt** personīgo datu ievades lauku ievākšanas un apstrādes apjomus
- **Samazināt** uzglabājamo personīgo datu apstrādes mūžu
- **Šifrēt datus** uzglabāj ot un kad tie tiek pārsūtīti
- **IP adrešu maskēšana** un padarīt anonīmu cita veida lietotāja datus
- **Samazināt** autorizēto darbiniku skaitu, kuriem ir piekļuve personīgajiem datiem
- **Palielināt** savas spējas samazināt un novērst draudus personīgajiem datiem

GDPR prasību izpilde

Tagad, kad esat iepazinušies ar idejām kā veidot GDPR prasībām atbilstošu organizāciju, tad noteikti plānojat kā tās īstenot pēc iespējas ātrāk un novērst esošos trūkumus, lai atbilstu visām prasībām un iekļautos termiņos. WatchGuard var palīdzēt sasniegt atbilstību regulai, izmantojot ļoti efektīvus datu aizsardzības tehnoloģiju risinājumus.

Bez tam, WatchGuard ir padarījis šo procesu pavisam vienkāršu. Pateicoties Total Security Suite uzlabojumam ir iespējams izpildīt GDPR prasības ar vienu vienīgu licenci, kas ļauj nodrošināt stipru un augstvērtīgu aizsardzību. WatchGuard Firebox® iekārta ar Total Security Suite nodrošina 16 no galvenajām 20 SANS Critical Security Controls (v6) un sniedz plašu produktu klāstu.

WatchGuard Firebox iekārta ar Total Security Suite nodrošina
16 no SANS **Top 20** Critical Controls prasībām

SANS Top 20 Critical Security Controls V6

CS1	Saraksts ar autorizētajām un neautorizētajām iekārtām	*Yes*
CS2	Saraksts ar autorizēto un neautorizēto programmatūru	*Yes*
CS3	Droša uzstādīšana uz mobilājām ierīcēm, darba stacijām, laptopiem un serveriem	*Yes*
CS4	Nepārtraukts ievainojamību novērtējums unto novēršana	*Yes*
CS5	Administratīvo tiesību kontrole	*Yes*
CS6	Uzraudzīt un analīzēt log datnes	*Yes*
CS7	E-pasta un internetapārlūka aizsardzība	*Yes*
CS8	Aizsardzība no ļaunprātīgas programmatūras	*Yes*
CS9	Ierobežojumi un kontrole pār tīklā esošajiem portiem, servisiem un protokoliem	*Yes*
CS10	Iespēja atgūt datus	*No*
CS11	Drošа tīkla iekārtu konfigurācija, tādām iekārtām kā ugunsmūri, maršrutētāji un komutatori	*Yes*
CS12	Aizsardzības ierobežojumi	*Yes*
CS13	Datu aizsardzība	*Yes*
CS14	Kontrolējama pieeja	*Yes*
CS15	Bezvadu tīklu piekļuves kontrole	*Yes*
CS16	Lietotāju profilu uzraudzīšana un vadība	*Yes*
CS17	Lietotāju drošības apmācības	*N/A*
CS18	Aplikāciju programmatūras drošība	*Yes*
CS19	Reaģēšana uz incidentiem un to vadība	*N/A*
CS20	Izplatības testi un Red Team apmācības	*N/A*

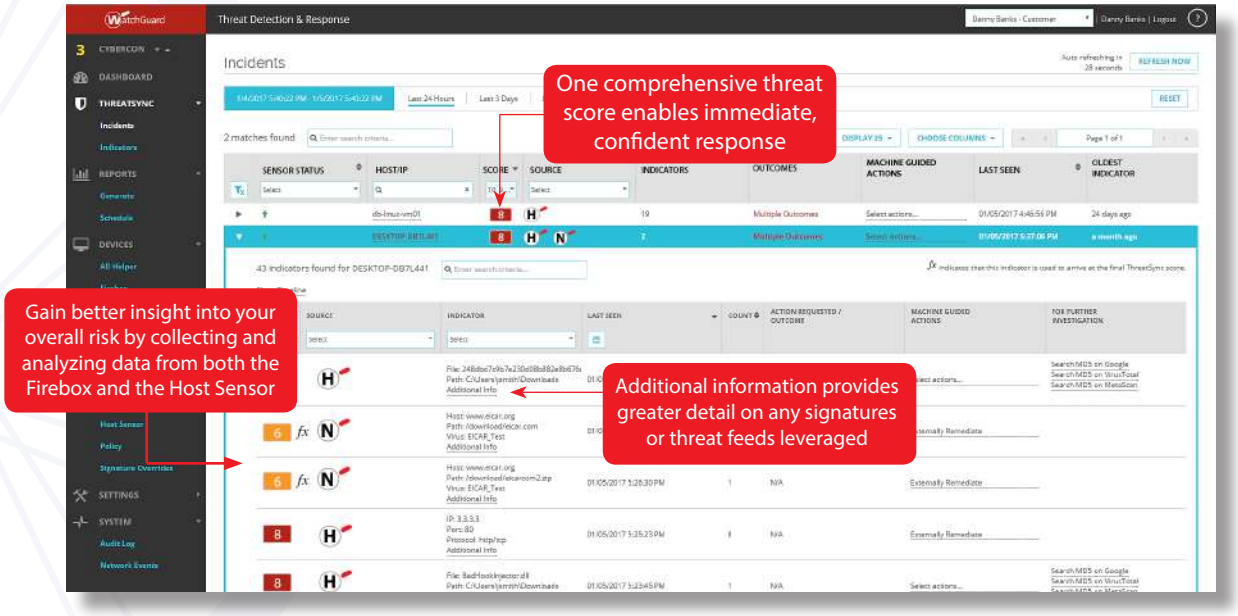


GDPR prasību izpilde

WatchGuard Total Security Suite piedāvā unikālus risinājumus, lai nodrošinātu īpašu atbilstību GDPR prasībām iekļaujot:

Threat Detection and Response (TDR) – GDPR pieprasa "situāciju apzināšanu", ko WatchGuard piedāvā ar savu īpašo ThreatSync iespēju. ThreatSync atlasa drošības informāciju no tīkla un gala iekārtām, lai vienkāršā veidā informētu par drošības incidentu izplatību.

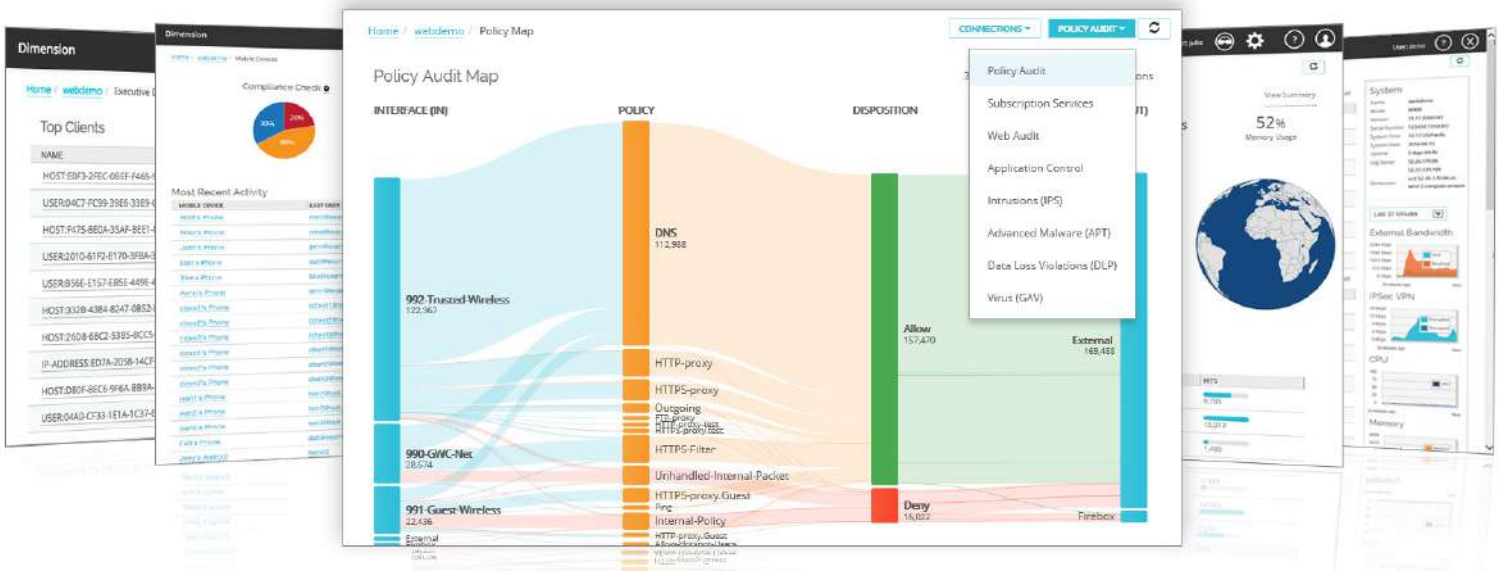
Turklāt, Jūs varat veidot drošības ierobežojumus, kas automātiski samazinātu riskus un būtu daudz efektīvāks risinājums par cita veida preventīvajiem pasākumiem. Līdz ko draudi tiek izolēti, informācija par to tiek nosūtīta uz WatchGuard centrālo sistēmu, kur tā t iek identificēta un tiek aizliegts atkārtoti iekļūt Jūsu tīklā. Ņemot vērā, ka TDR ir mākoņ-bāzēts risinājums, tad Jums ir iespēja izvēlēties, ka Jūsu dati tiek glabāti ES un tas nodrošina GDPR datu pārsūtīšanas panta izpildi.



Threat Detection & Response

WatchGuard Dimension™ – Šis rīks ļauj ātri iegūt pārskatāmu un jēgpilnu log datu informāciju un atskaites, kas atbilst regulas prasībām. Tas piedāvā plašu datu pārskatu un atskaišu sistēmu, kas spēj identificēt galveno informāciju par tīkla drošības problēmām un tendencēm, paaugstinot spējas cīnīties pret draudiem, atklājot visas ar drošību saistītās darbības tīklā.

Vēl šis rīks piedāvā efektīas lietotāju anonimizēšanas iespējas, kas spēj aizvietot visu personīgi identificējamo informaciju (PII) atskaitēs un ziņojumu panelī, kur tā tiek aizstāta ar šifrētiem iniciāļiem. Šādā veidā tiek aizstāti lietotāju vārdi, IP adreses, resursa nosaukumi un mobilo iekārtu nosaukumi ar nejauši izvēlētiem simboliem, kas nodrošinās maskētu datu pārsūtīšanu.



WatchGuard Dimension



GDPR prasību izpilde

Encryption & VPN – Vispareizākā rīcība ir personīgos datus turēt šifrētus gan glabājot, gan pārsūtot, kas samazinās riskus. WatchGuard Firebox UTM risinājums piedāvā drag-and-drop VPN izveidi starp attālināti saistītiem ofisiem. To ir ļoti ātri un vienkārši izveidot. Turklāt tas ir drošs un stabils risinājums, kas ir būtiski, ja Jūsu bizness ir atkarīgs no nepārtrauktas un drošas datu pieejamības.

WatchGuard Firebox, izmantojot VPN funkcijas, tīkla uzraudzīšanu, lietotāju anonimitāti ar Dimension iespējām, TDR automātisko apdraudējumu novēršanu, spēs pilnībā sasniegt un nodrošināt GDPR prasībām atbilstošu drošības risinājumu.



The First Man to Cycle through the Eurotunnel
Photo by: Chris Froome

WatchGuard Total Security Suite

GALVENIE DROŠĪBAS PAKALPOJUMI

INTRUSION PREVENTION SERVICE (IPS)

REPUTATION ENABLED DEFENSE SERVICE (RED)

SPAMBLOCKER

GATEWAY ANTIVIRUS (GAV)

WEBBLOCKER URL FILTERING

NETWORK DISCOVERY

APPLICATION CONTROL

UZLABOTIE DROŠĪBAS PAKALPOJUMI

APT BLOCKER – ADVANCED MALWARE PROTECTION

DATA LOSS PREVENTION (DLP)

THREAT DETECTION AND RESPONSE

DIMENSION COMMAND



GDPR veicamo darbu saraksts

Lai palīdzētu Jums, esam sastādījuši sarakstu ar veicamajām lietām ar kurām būtu jāsāk. Šis protams nav pilnīgs saraksts, un to būtu vēlams īstenot izmantojot arī citus risinājumus, lai pārliecinoši atbilstu GDPR prasībām.

☑ ES pilsoņu personālo datu identificēšana.

- Kādi personīgie dati ir ievākti un/vai tiek apstradāti?
- Kur dati tiks glabāti vai pārsūtīti? Un cik ilgi?
- Kādas uzgalbāšanas politikas un procesi tiek piemēroti datiem? Vai šos procesus var samazināt?
- Vai šie dati būs Jūsu pārraudzībā, vai nolīgtā datu pārziņa pārraudzībā?
- Vai šie dati paliks ES visu laiku?

☑ Aprakstiet labprātīgas piekrišanas informāciju un procesu, kas notiek ievācot datus.

- Vai personai pirms piekrišanas par datu ievākšanu un apstrādi ir skaidri izklāstīti visi nosacījumi?
- Vai piekrišana dota datu ievākšanas brīdī?
- Vai pirms piekrišanas tiek sniegta informācija par datu turētājs, datu apstrādātāju un datu aizsardzības pārzini (DPO), ja tāds ir nozīmēts?
- Vai tiek aprakstīts datu apsrādes mērķis, apstrādes drošums un juridiskais pamatojums?
- Vai tiek norādīts periods,cik ilgi dati tiks glabāti?
- Vai tiek minēti datu saņēmēji vai datu saņēmēju grupas ?
- Vai ir izskaidrotas personas tiesības piekļūšanai saviem datiem, labot, pieprasīt datu dzēšanu vai padarīt datus pārvietojamus, kā arī personas tiesības vērsties ar sūdzībām uzraudzības iestādēs?
- Vai ir norādes uz to, ka dati nonāks arī ārpus ES?
- Vai ir noteikts, ka datu ievākšana ir obligāta vai brīvprātīga, un kādas ir sekas, ja prasītie dati netiek iesniegti?
- Vai piekrišanu atsaukt ir tikpat vienkārši kā dot piekrišanu?

☑ Aprakstiet saziņas iespējas ar personas datu īpašniekiem.

- Kā datu īpašnieks varēs piekļūt, labot, dzēst un apkopotā veidā saņemt savus datus, lai tos varētu pārvietot?
- Kā datu īpašniekam atsaukt savu piekrišanu?
- Kā organizācija informēs datu īpašnieku gadījumā, ja notikusi datu noplūde?

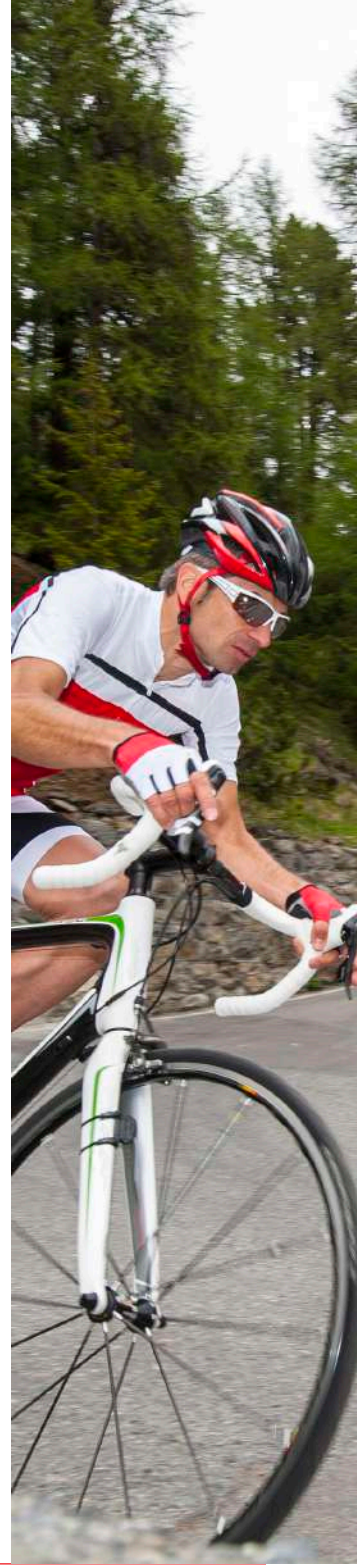
Noteikt, vai šī brīža datu uzglabāšanas nosacījumi un datu apstrādes politikas ir atbilstošas.

- Kur tiek glabāti dati par personas piekrišanu datu uzglabāšanas noteikumiem?
- Vai pastāv kāda veida ieraksti vai log dati par procesiem, kas skar personas datus?
- Vai piekļuve šo ierakstu vaicājumiem, meklējumiem un atskaitēm ir droša un tiem var piekļūt tikai autorizēts personāls?
- Vai noteikumi, kas apraksta datu apstrādes procesu, regulāri tiek parskatīti un atjaunoti un vai tas notiek saskaņā ar regulu?
- Ja par šiem datiem atbildīgais atrodas ārpus ES, vai ir nozīmēts pārstāvis ES, un vai tas tiek dokumentēts?
- Ja tiek noslēgts līgums par datu apstrādi, vai līgumā ir iekļauti visi nepieciešamie notekummi, atbilstoši GDPR nosacījumiem, kas nodrošina drošu personas dat u apstrādi?
- Vai ir pietikama piekļuves kontrole ēkai un serveriem, lai novērstu nepiederošu personu piekļuvi personu datiem?

Noteikt, vai datu aizsardzības metodes un tehnoloģijas ir pietiekamas un atbilstošas GDPR noteikumiem?

- Vai ir veikti atbilstoši tehniskie un organizatoriskie pasākumi, lai nodrošinātu datu aizsardzību pret nejaušu vai nelikumīgu iznīcināšanu, zudumu vai pārveidošanu, un neatļautu vai nelikumīgu uzglabāšanu, apstrādi, piekļuvi vai tālāk izpaušanu?
- Vai drošības noteikumi paredz:
  - kā pasargat datus uzglabājot un pārsūtot
  - kā atgūt datus, kad tiek liegta un/vai apgrūtinata pieejamība datiem
  - kā tiek nodrošināta savlaicīga risku apzināšanās un nodrošinātas nekavējošas darbības risku novērsošanai, koriģējošanai un problēmu mazinošanai pret ievainojamībām vai konstatētam incidentam, kas spētu radīt apdraudējumu datiem
  - vai tiek aprasktīts process kā notiek regulāra drošības politiku efektivitātes pārbaude
- Vai tiek aprakstīs process, kas nodrošina paziņojumu par incidentu 72 stundu laikā kopš ielaušanās?
- Vai ir veikts Datu aizsardzības ietekmes novērtējums (DPIA), kas novērtētu to, vai datu apstrādes process var radīt konkrētus riskus? Vai tas ir veikts pēdējo 2 gadu laikā, vai uzreiz pēc tam, kad tika veiktas izmaiņas specifisku risku apstrādes procesā?
- Vai ir iecelts Datu aizsardzības pārzinis (DPO)?

Atbildot uz šiem jautājumiem, Jums palīdzēs identificēt un saprast, kur ir nepilnības un spēt savlaicīgi tās novērst pirms nav par vēlu!





Lai uzzinātu vairāk, apmeklējiet www.watchguard.com

SIA Maksikoms
Tel: +371 29459183
E-pasts: info@maxicom.lv

Jānis Dambis
Tel: +371 25405544
E-pasts: janis.dambis@maxicom.lv

Aleksejs Petrovs
Tel: +371 29618573
E-pasts: aleksejs.petrovs@maxicom.lv

1. http://www.eugdpr.org/
2. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
3. https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Limitation of warranties: The information in this document is provided "as is" without any representations or warranties, express or implied. Professional assistance: You must not rely on the information in this document as an alternative to legal advice. If you have any specific questions about any legal matter you should consult your attorney or other professional legal services provider.

©2017 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE66998_031017