ALIMENTATION

COUCHE-TARD INC.

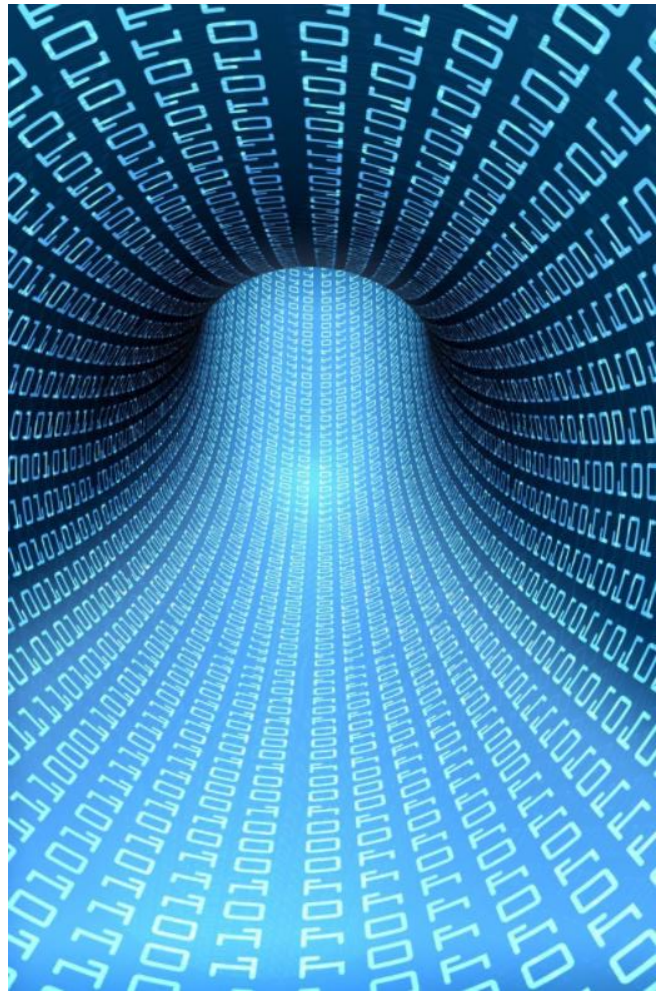
ISIKUANDMETE KAITSE VALGUSES JA VARJUS

DIANA VEIGEL

10.05.2018

ISIKUANDMED

ISIKUANDMED on TÄNA valuuta (inimese nimi, telefoni number või e-maili aadress jne), mis rändavad kontrollimatult käest kätte, ettevõttest ettevõttesse ja igasugune arusaamine ja kontroll puudub, kes, kus ja milleks neid kasutab.



GDPR'GA EI LEIUTATA JALGRATAST

Varem tuli meil Eestis lähtuda kahest dokumendist:

- 01.01.2005 jõustunud Elektroonilise side seadusest ning
- 01.01.2008 jõustunud Eesti Isikuandmete kaitse seadus

PEAMISED VÄLJAKUTSED

- **Juurdepääsuõigus** - andmesubjektil on õigus näha töödeldavaid andmeid.
- Isikuandmete **töötlemiseks vajalik õiguslik alus** - kui seadus ei sätesta teistsugust õiguslikku alust, tuleb andmesubjektilt küsida nende nõusolekut andmete töötlemiseks.
- Andmete **korduvkasutamine -** ühe eesmärgi jaoks kogutud andmeid ei saa vabalt teise jaoks uuesti kasutada.
- EL andmete **väljastamise keeld** - kui see pole erilistel alustel, on andmete edastamine väljaspool ELi keelatud.

JA NII SEE ALGAS…

14.04.2016 kiitis Euroopa Parlament heaks Isikuandmete kaitse üldmääruse. Uus määrus on otsekohalduv, mis tähendab, et koos siseriiklike rakendusaktidega hakkab see asendama ka Eesti isikuandmete kaitse seadust.

Määrus jõustus 24.05.2016 ning seda hakatakse kohaldama pärast kaheaastast üleminekuaega, alates **25. maist 2018. a.**

GDPR TUGISAMBAD

Vastutava töötleja kohustused

Andmesubjekti ehk isiku õigused

Info turvalisus ja selle tagamine

5 LÄHTEKOHTA

Lihtsam juurdepääs andmetele

- Kõigil klientidel on õigus täpselt teada, mida kogutakse ja mida nende andmetega tehakse.
- Koostage dokument, kus kirjeldate milleks kogutakse ja kuidas kliendiandmeid kasutatakse.
- Edastage selge info kliendile millal ja kuidas andmed töödeldakse ja kustutakse (lepingus, tingimustes, reeglites kodulehel jne).

Andmete säilitamine ja nende liikuvus

- Kõikidel klientidel on õigus saada infot mida ettevõtte nende kohta omab, kuidas säilitab ja mida nende andmetega tehakse.
- Kogu kliendiinfo ja andmed peab olema säilitatud viisil, mis võimaldab seda sooviavalduse saamisel kustutada, saata seda kolmandale osapoolele või edastada kliendile.

Õigus olla unustatud ehk kustutatud

- Kliendil on õigus igal ajahetkel oma nõusolek andmete töötlemiseks tagasi võtta ja nõuda oma andmete kustutamist.
- Kogu kliendiinfo peab olema säilitatud ja ligipääsetav kujul, mis võimaldab kogu isikuga seotud info kustutamist vastava soovi saamisel.

Taasesitatav nõusolek töötlemiseks ja kommunikatsiooniks

- Ettevõtte peab suutma tõendada, et neil on nõusolek isiku teabe säilitamiseks, kliendiga kommunikeerimiseks jne. Täna, aasta pärast ja ka kümne aasta pärast.
- Kogu ja salvesta kliendi nõusolek andmete töötlemiseks ning ka kommunikatsiooni saamise ja eelistuste kohta.

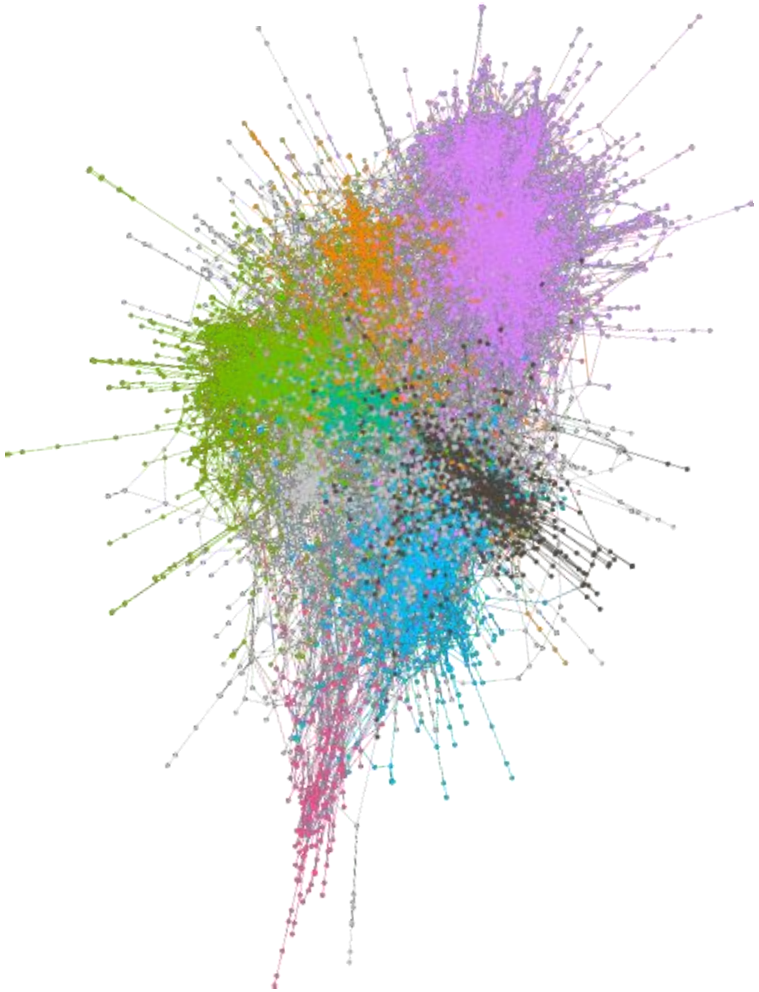
Minimaalselt andmeid

- Ainult eesmärgiga ja äriga seotult vajalik info kogutakse ja säilitatakse.
- Ennem vähem kui rohkem! Küsi, kas kõigel sellel infol, mida säilitakse ja kogutakse on eesmärk ja vajadus ettevõttes?
- Kõik mis ei ole vajalik ja mõistlik, tuleks kustutada!

ANDMETE TÖÖTLEMINE

Isikuandmete töötlemine = nende kogumine, analüüsimine ja kustutamine. Ka andmete vaatamine ja neile ligipääsu võimaldamine loetakse andmete töötlemiseks.

- Andmeid tohib töödelda ainult kindlaksmääratud eesmärkidel.
- Kliendile peab olema selgelt sätestatud ja edastatud/nähtavad/kättesaadavad andmete töötlemise eesmärgid
- Eesmärk peab olema üheselt mõistetav ega tohi olla liiga lai ega ebamäärane (nt "ameti ülesannete täitmine" jt)



KUIDAS MEIE ALUSTASIME

Andmekogude kaardistamine ja mõjuhinnang.

Määratle kõik andmete töötlemisega kaasnevad riskid (kus on andmed, kuidas neid käsitletakse, kelle on ligipääs, kuidas liiguvad ja mis nendega tehakse).

Kontrolli vastavust GDPR'le.

Kontrollisime üle kõik ettevõttes juba kehtestatud andmekaitsega seotud protsessid, blanketid/lepingud, süsteemid, infomaterjalid jne.

Kontrolli dokumentide ja andmete säilitamist ja vastavust.

Säilita täpselt niipalju kui isikuga sõlmitud lepingu täitmiseks on vaja ja täpselt nii kaua kui vaja! Kustutasime kõik vanad andmed mida ei kasutanud

Määra ettevõttes andmekaitse spetsialisti (DPO).

Isik, kes teab isikuandmete kaitsest, tehnilistest lahendustest palju, kuid samas ei puutu ise igapäevatöös isikuandmete ja nende töötlemisega kokku

DOKUMENDID, MIDA PEAKS KOOSTAMA

- ✓ Kaardistada ja määratleda andmekogud ja andmetega kaasnevad riskid (sisemine vaade)
- ✓ Isikuandmete käitlemise register (sisemine vaade)
- ✓ Privaatsuspoliitika ehk isikuandmete hoidmise reeglistik kus sõnasta mida, millal, kuidas ja kes andmetega teeb ehk andmehoidmise ja **-töötlemise põhimõtted** (välimine vaade)
- ✓ Volitatud/vastutava töötleja leping (kui kasutad **väliseid partnereid**)

DOKUMENDI REGISTER

BU	Department	Location	Content type category (eng)	Content (local language)	If personal data (choose sub category)	Reason of data processing	Media type	Data source (describe)	Storage facility	Sensitive Yes/No	Retention period
	Kus osakonnas?	Station/Office/ Riga									
BACE EE	CS	Office	Customer complaints	**Kliendikaebused**	C	Management of customer complaints	E	E-mail, Call Center	Lotus Notes, Teamsite, JDE	Yes	3 years
BACE EE	CS	Office	EXTRA card requirements	**EXTRA taotlused**	C	To help customers to join EXTRA Club	E;P	E-mail, Call Center, Stations	Outlook, Facebook	Yes	3 years
BACE EE	CS	Office	Reports	**Erinevad kliendipõhised väljavõtted ja raportid**	C	For statistical purposes	E	BI	Outlook, TeamSite	Yes	3 years
BACE EE	CS	Office	List of B2E customers	**B2E avaldused ettevõtete töötajatele**	C; E	based on B2E the offer	E	From B2B companyes	Outlook, Saurus	Yes	Untill B2B contact is valid for
BACE EE	CS	Office	List of CK emplyees with OMA level discount	**EXTRA Club personalisoodustuse taotlused**	E	To add OMA level discount for CK employees	E	Station manager/emplyee	Outlook, TeamSite, WMCard	Yes	Untill employment contract is valid
BACE EE	CS	Office	B2C payment and prepayemnt card offer	**B2C maksekaardi lepingud**	C	To fullfill B2C paymentcard agreement	E	leping.ee website, Saurus	Saurus, TeamSite	Yes	Untill B2C contact is valid for
BACE EE	CS	Office	Posting report from Oberthur to Omniva and CK	**Omniva posting report**	C	To send CK cards to customers	E	Copy from customer contact	Outlook, TeamSite,Wmcard/PALS	Yes	Untill B2B contact is valid for
BACE EE	CS	Office	PALS invoice XML file	**Fitek arved**	C	Monthly invoicing for customers	E	GMC file via secured server to Fitec	UCM, Arved.ee; Card e-service	Yes	Untill B2B contact is valid for
BACE EE	CS	Office	Automatstation money refunds	**Automaatjaamade tagasimakse avalduste süsteem**	C	Refund money for customers if error occured	E	Form from website	Saurus, Outlook	Yes	1 year
BACE EE	CS	Office	Video monitorings ordered by B2B customers or authorities	**Videopäringute väljavõtted**	C	Request regarding fraud cases	E	E-mail	Outlook	Yes	
BACE EE	Stations	Office/Stations	Incident reports from stations	**Insidendiraportid**	C	Customer complaints management	E;P	Stations, CC, JDE	Outlook, JDE	Yes	
BACE EE	CS	Office	access to CK customer data	**Koostöö kõnekeskusega (Runway)**	S	service for CK customers	E	Outlook, Call	Outlook	Yes	
BACE EE	CS	Office	Requests from diff. authorities	**Päringud ametiasutustelt (TKA, PPA, MTA)**	C	Request regarding fraud cases	E	E-mail	Outlook	Yes	

ISIKUANDMED JA CIRCLE K TURUNDUS

Isikuandmed on uues seaduse võtmes defineeritud väga laiapõhjaliselt ja põhimõtteliselt on need kõik andmed, mis puudutavad füüsilist isikut ja mida me turunduses erinevatel eesmärkidel kasutame (e-mail, telefon, nimi, aadress, sünniaeg või ID kood jne.).

Toon ära mõned valdkonnad, kus meie töötleme isikuandmeid:

- Lojaalsusprogramm Circle K EXTRA Club
- Turunduslike mängudes ja aktiviteetides
- Turvakaamerate salvestised teenindusjaamades
- E-kirjad ja muud päringud klientidelt klienditeenindusse
- Personaliosakonnas töötajate ja kandideerijate andmed

LOJAALSUSPROGRAMM JA GDPR

Circle K EXTRA on üks vanemaid Eesti lojaalsusprogramme enam kui 200 000 kasutajaga.

Klientidel on võimalus programmis osaleda kas lojaalsuskaardiga, Partnerkaardiga või SEB ja Swedbanki pangakaardiga.

Peamised väljakutsed meie jaoks olid:

- *Kliendid on oma nõusolekuid ja andmeid meile andnud enam kui 20 aasta jooksul.*
- *Oleme enamus aastaid kogunud klientide andmeid ja kommunikatsiooni nõusolekuid pabervormidel.*
- *Lojaalsusprogrammi reeglid/leping tuli viia vastavusse GDPR'ga*

UUED TINGIMUSED- UUS LEPING

Mida uued lojaalsusprogrammi tingimused selgelt sõnastavad ehk mida me lisasime või uuendasime lepingus:

- Nõusolek isikuandmete töötlemiseks ja kuidas nõusolek tagasi võtta.
- Andmete töötlemise eesmärk ja andmesubjekti õigused (õiguste teostamine ja juurdepääs andmetele).
- Kommunikatsiooni eesmärgid ja kuidas klient saab oma eelistusi muuta.
- Andmete kogumine ja säilitamine – ostude registreerimine (tšekk 30 päeva) ja millal andmeid üldistuvad, delikaatsete ostude mitte registreerimine. Krüpteerimine.
- Andmete kustutamine (poolikud kontod 150 päeva, passiivikud 24 kuu pärast)

KAHEASTMELINE IDENTIMINE

Et olla veendunud andmete õiguses ja saada kinnitus, mis tõestaks kliendi nõusolekul andmete töötlemiseks on oluline kasutada kaheastmelist identimist.

Meie lahendus: andmesubjekt täidab oma andmed veebisaidil ja seejärel saadame kinnitus koodi, millega klient kinnitab, et andmed on õiged ja just tema antud ja selle sama koodiga saab ta kinnituse andmete käitlemiseks.

Nõustun tingimustega ja siis valin kommunikatsiooni- ja suhtluskanali(d).

NÕUSOLEK JA EELNEVALT TÄIDETUD VORMID

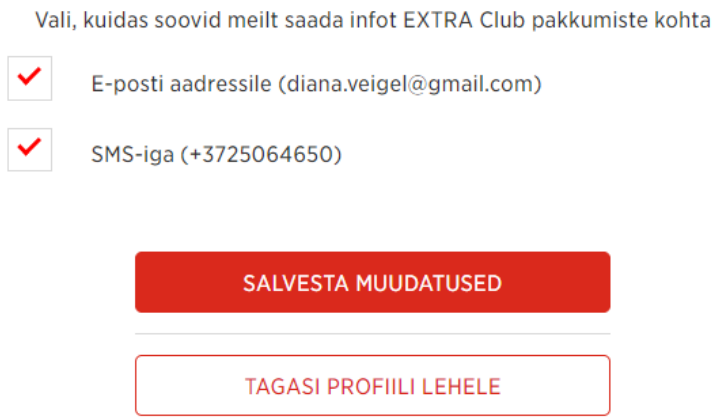
Uue regulatsiooni järgi on vajalik ühene ja selgesõnaline nõusolek uudiskirja/kommunikatsiooni saamiseks.

See tähendab, et:

- opt – out nõusolek ei ole enam vastavuses uue määrusega ehk eelnevalt nn automaatselt ära „linnutatud“ kast ei ole nõusoleku andmine.

GDPR vaates on vajalik opt-in ehk kliendi enda tahteavalduse vormistamine ehk klient annab selgesõnaliselt teada milliseid kanaleid pidi ta soovib, et ettevõte temaga suhtleb.

NB! Kui EI OLE nõusolekut kommunikatsiooniks, ära suhtle!



LOOBUMINE JA KUSTUTAMINE

Kliendil on igal ajahetkel õigus oma nõusolek nii programmis osalemiseks, kui andmete töötlemiseks ja kommunikatsiooniks tagasi võtta. Sooviavalduse vorm on alati **KIRJALIKUS TAASESITAVAS** vormis.

- Kommunikatsioonist loobumise link uudiskirjas, SMS-l ja kodulehel selleks võimalus ühe nupule vajutamisega.
- Loobumise puhul on oluline , et need soovid ka reaalselt kliendi andmete juurde märgitud saaksid ja järgmisel korral neid ka täidetakse.
- Oluline on kommunikatsioonis eristada ka kanaleid – kliendil peab olema võimalus oma eelistus teha.

KUSTUTAMISEL ERIJUHUD

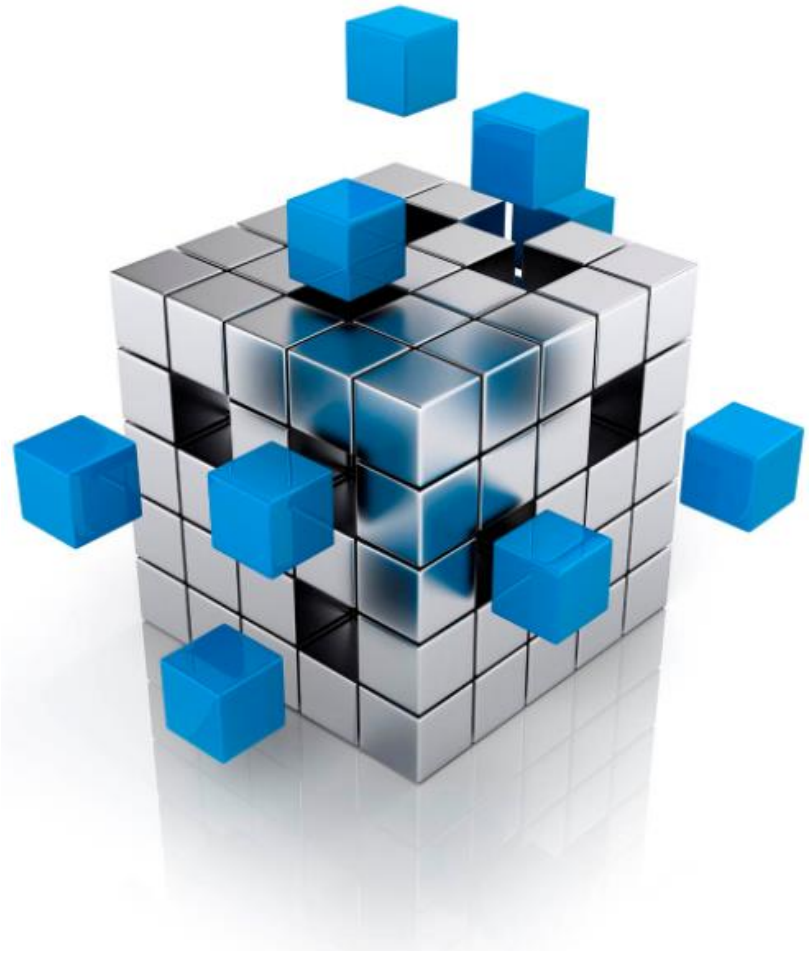
- Isiku õigus nõuda andmete kustutamist **EI OLE ABSOLUUTNE.**
- Kui seadus on andnud andmete töötlejatele nende säilitamiseks teised piirid, siis andmeid ei pea kustutama – arved, raamatupidamisdokumendid jms.
- Kuid turunduse ja reklaami eesmärgil andmed tuleb ALATI kustutada.

VORMID JA PROTSESSID

Tegime endale konkreetsed vormid, rutiinid ja protsessid lähtudes uuest määrusest.

Peamised muudatused:

- Millised on uued protsessid, kui klient soovib oma andmeid kustutada.
- Millised on protsessid, kui klient soovib ülevaadet millised andmed meil on ja neid näiteks ka elektrooniliselt saada (vorm, protseduur jne).
- Kui meie poole pöörduvad õiguskaitseorganid (politsei, kindlustus jne).
- Videopäringute väljavõtted (kellele ja kuidas edastame)



KUS ON SINU KLIENDI ANDMED?

Kui klienti palub kustutada oma andmed, näha nõusolekut? Hakkame otsima:

- Kellegi arvutis Excelis?
- Kuskil laoruumis paberkandjatel kastides?
- Kellegi kapis või sahtlis kaustas?
- Kuskil varukoopias.

Info turvaline säilitamine on A ja O. Andmed peavad olema krüpteeritud. Krüpteering peab olema kasutusel, kus tehnoloogiliselt võimalik. Kui krüpteerimine ei ole võimalik, on vajalik muid turvalisuse võtmeid kasutada (oluline on kaotada seos inimese ja detailse data vahel).

<E0><98>_^R<F6>Z̧SC.<E0><94>k`4^^Et'<
E6><83>|<FC><F
C><D0><EA>H<8E>0B(2)<A9>;s^U<DF>8^
?Y<BD><8A>rr!<E
E>:<B6>x<BA>O,<F4>^XT<DE>A<:n

KODULEHEL REGAMINE, TARBIJAMÄNGUD, AUTOMAATIKA

- Tihti kohtab, et tarbijamängudeks kogutud andmeid kasutatakse ka hilisem turunduses. See **EI OLNUD** enne OK ja ei ole ka tulevikus. Tarbijamängu andmed on vaid selle konkreetse mänguga seotud ja hiljem tuleb andmed kustutada.

- Visiitkaart messilt lisainfo saatmiseks ja kodulehel kasutajaks registreerimine lisainfo saamiseks, toote ostmine webist ja tarbijakampaaniasse registreerimine isikuandmetega jne **EI ANNA ÕIGUST** kliendile reklaami ja kommunikatsiooni saata.

- Automatiseeritud otsuste puhul pead olema võimeline **selgitama kliendile algoritmi mille alusel otsus tehakse** (nt krediidiotsused, mille puhul kliendi krediidikõlbulikkust hinnatakse).

OSTAME TEENUSE SISSE?

Kõik lepingud, mis sõlmitakse kolmandate osa-pooltega ja mis hõlmavad isikuandmete töötlemist (kliendiprofileerimine, otsepostitused, kampaaniate korraldamine jne) peavad olema selged ja kirjalikud ning lepingus peab olema selgelt määratletud vastutus.

OLULINE: Andmete koguja on alati VASTUTAV TÖÖTLEJA!

MIS UUENDUSED MEIE TELLISIME

Mõned näiteks tehnilistest lahendustest ja uuendustest mida me lojaalsusprogrammi webis tegime:

- et klient saaks lihtsalt loobuda kliendiprogrammis osalemisest ja olla õigus unustatud, selleks ei ole vaja enam saata kirja, vaid piisab oma kontol ühele nupule vajutamisest ja kinnitusest
- et kõik uudiskirjad, SMS-id jms sisaldaksid „loobumise“ nupukest jne
- uuendasime videovalve ja salvestamiste silte ja teavitusi teenindusjaamas.
- lõime protsessid ja vormid päringute ja soovidega tegelemiseks
- koolitasime oma klienditeenindajaid ja uuendasime töö sisekorra eeskirjasid, e-koolitused kontorile ja teenindusjaamadele

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

KOKKUVÕTVALT

- ✓ Vii oma andmete töötlemine vastavusse seadusega. Kus hoiad, mida kogud, piira ligipääsud, sätesta lepingus ja tee andmebaasid korda.
- ✓ Kõik kliendi andmed, tehinguinfo jms peab olema taas-esitavas vormis. Ära riski mõttetult.
- ✓ Veendu, et suudad kliendi andmeid edastada. Määratle andmete säilitamise detailsus ajas.
- ✓ Kontrolli nõusolekut suhtluseks. Anna valik ja suhtle vaid siis kui on aktiivne nõusolek ette näidata.
- ✓ Tööta välja kontrolli rutiinid, sea vastutavad isikud ja vii läbi auditeid, et kõik päriselt ka töötab.
- ✓ Taga, et kõik klientide tehtud muudatused oma andmetes oleks uuendatud ja ajakohased.
- ✓ Taga protsesside töökorras olek ka aasta pärast. Rutiinsed kontrollid, järjepidevus on siin võtmesõnad.

Tänan.

Küsimusi?