Dokumentų sąrašas

	DOKUMENTO PAVADINIMAS	KOMENTARAS	+ / -
		ASMENS DUOMENŲ TVARKYMO TAISYKLĖS	
1.	Asmens duomenų tvarkymo taisyklės	Pagrindinis dokumentas, kurį privalo turėti kiekviena įstaiga. Šiame dokumente numatomos priemonės, kurios užtikrina tinkamą atitiktį Bendrajam duomenų apsaugos reglamentui (toliau – BDAR).	
		SANTYKIAI SU DUOMENŲ VALDYTOJAIS IR TVARKYTOJAIS	
2.	Sutartis su duomenų tvarkytoju	Tai būtinas dokumentas, jeigu įmonėje turite sutarčių su IT, buhalteriais ir panašiai.	
3.	Sutartis su bendrais duomenų valdytojais	Kai du ar daugiau duomenų valdytojų kartu nustato duomenų tvarkymo tikslus ir priemones, jie yra bendri duomenų valdytojai. Tokiu atveju, tarpusavio susitarimu bendri duomenų valdytojai privalo nustatyti savo atitinkamą atsakomybę už pagal BDAR nustatytų prievolių vykdymą.	
		SANTYKIAI SU DARBUOTOJAIS	
4.	Pranešimas apie tvarkomus asmens duomenis	Darbdavys turi informuoti darbuotojus apie jų asmens duomenų tvarkymą glausta, skaidria, suprantama ir paprasta kalba.	
5.	Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarka	Darbdavys privalo išsamiai dokumentuoti informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos tvarką: kokie darbuotojai, kokiais atvejais ir kokiomis sąlygomis bus stebimi. Darbuotojai turi būti pasirašytinai ar kitu informavimo faktą įrodančiu būdu supažindinti su tokia tvarka, kuri turi būti aiški, kad darbuotojai suprastų jų asmens duomenų tvarkymo apimtį ir galimas pasekmes.	
6.	Sutikimas dėl atvaizdo naudojimo	Jei darbuotojo atvaizdas bus publikuojamas viešai (pvz., internetinėje svetainėje), darbdavys turi gauti darbuotojo sutikimą dėl atvaizdo naudojimo.	
7.	Sutikimas dėl gimimo datos skelbimo, viešo sveikinimo su gimtadieniu	Darbuotojų gimimo data gali būti skelbiama viešai ir (ar) darbuotojas sveikinamas su gimtadieniu tik turint išankstinį jo sutikimą.	
8.	Interesų pusiausvyros testas dėl darbuotojų el. komunikacijos stebėjimo	Darbdavys, norėdamas vykdyti darbuotojo stebėseną, įprastai turėtų atlikti interesų pusiausvyros testą, kad įsitikintų, ar darbdavio interesai persveria darbuotojo interesus bei pagrindines teises ir laisves. Šiuo atveju, darbuotojo stebėsena negali būti pagrįsta darbuotojo sutikimu (dėl darbdavio ir darbuotojo santykiams būdingos priklausomybės).	
9.	Poveikio duomenų apsaugai vertinimas, jei vykdoma darbuotojų el. komunikacijos stebėsena	Poveikio duomenų apsaugai vertinimas (toliau – PDAV) privalo būti atliktas kuomet darbuotojų asmens duomenys tvarkomi darbuotojo stebėsenos ar kontrolės tikslais. Atliekant PDAV turėtų būti išsamiai įvertinti galimi pavojai ir priemonės pavojaus valdymui.	
10.	Sutikimas dėl kandidato asmens duomenų saugojimo	Kandidatų į darbo pozicijas gyvenimo aprašymai gali būti saugomi tik tuo atveju, jei yra gautas išankstinis asmens sutikimas. Kitu atveju, pasibaigus konkrečios pozicijos darbuotojų atrankai, neatrinktų kandidatų gyvenimo aprašymai turi būti nedelsiant sunaikinti.	

INTERNETINĖ SVETAINĖ			
11.	Privatumo politika	Kiekviena organizacija, tvarkanti internetinę svetainę, joje turėtų paskelbti pranešimą dėl asmens duomenų privatumo.	
12.	Sutikimas dėl slapukų	Jeigu svetainėje yra naudojami slapukai, tai yra būtina apie juos informuoti visus svetainės lankytojus. Tai yra, atsidarius internetinės svetainės langą, turi atsirasti pranešimas apie naudojamus slapukus.	
ASMENS DUOMENŲ PAREIGŪNAS			
13.	Asmens duomenų pareigūno pareiginė instrukcija	Duomenų apsaugos pareigūną privalo paskirti valdžios institucijos ir įstaigos bei kitos organizacijos, kurių pagrindinė veikla yra dideliu mastu sistemingai stebėti asmenis arba dideliu mastu tvarkyti specialių kategorijų asmens duomenis (pavyzdžiui sveikatos asmens duomenys).	
14.	Sutartis su asmens duomenų pareigūnu	Duomenų apsaugos pareigūnas savo pareigas gali eiti ir nedirbdamas duomenų valdytojo ar duomenų tvarkytojo organizacijoje, o veikiant pagal paslaugų sutartį. Todėl yra būtina atskira sutartis.	
TELEFONINIŲ POKALBIŲ ĮRAŠINĖJIMAS			
15.	Telefoninių pokalbių įrašymo taisyklės	Telefoninių pokalbių įrašymas turi būti reglamentuotas duomenų valdytojo rašytinės formos dokumente. Darbuotojai telefoninių pokalbių įrašymo atvejais turi būti informuojami apie tai, kokiu tikslu bus vykdomas telefoninių pokalbių įrašymas, kada ir kokie pokalbiai bus įrašomi, kas ir kokiais atvejais juos perklausys ir pan.	
16.	Teisėto intereso vertinimo testas dėl telefoninių pokalbių įrašymo	Įmonė norėdama įrašyti darbuotojų pokalbius su klientais ir (ar) potencialiais klientais, turėtų atlikti interesų pusiausvyros testą, siekdama įsivertinti, ar jos interesai persveria darbuotojo interesus, pagrindines teises ir laisves.	
17.	Poveikio duomenų apsaugai vertinimas dėl telefoninių pokalbių įrašymo	Poveikio duomenų apsaugai vertinimas privalo būti atliekamas, kai vykdomas telefoninių pokalbių įrašymas.	
VAIZDO STEBĖJIMAS			
18.	Vaizdo stebėjimo taisyklės	Duomenų valdytojas turi pateikti duomenų subjektui visą informaciją, kuri užtikrintų sąžiningą ir skaidrų duomenų tvarkymą, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes.	
19.	Teisėto intereso vertinimas dėl vaizdo stebėjimo	Įprastai vaizdo stebėjimas vykdomas remiantis teisėto asmens duomenų tvarkymo sąlyga – savo teisėtų interesų siekimu. Kai remiamasi šia sąlyga, reiktų įvertinti teisėtus duomenų valdytojo interesus ir poveikį duomenų subjekto interesams. Taip pat reikėtų periodiškai iš naujo įvertinti teisėto intereso buvimą bei būtinybę vykdyti stebėseną (rekomenduojama kartą per metus, priklausomai nuo aplinkybių).	
20.	Poveikio duomenų apsaugai vertinimas dėl vaizdo stebėjimo	Poveikio duomenų apsaugai vertinimas privalo būti atliekamas, kai vaizdo stebėjimas vykdomas patalpose ir (ar) teritorijose, kurios nėra duomenų valdytojo valdomos nuosavybės ar kitais teisėtais pagrindais; sveikatos priežiūros, socialinės globos, įkalinimo įstaigose ir kitose įstaigose, kuriose paslaugos yra teikiamos pažeidžiamiems asmenims; kartu su garso įrašymu; darbuotojų asmens duomenų tvarkymas stebėsenos ar kontrolės tikslais;	

		asmens duomenų tvarkymas dideliu mastu, kai asmens duomenys gaunami ne iš duomenų subjekto.	
21.	Informacinė lentelė apie vykdomą vaizdo stebėjimą	Duomenų subjektai turėtų žinoti apie tai, kad vykdomas stebėjimas vaizdo kameromis. Juos reikėtų išsamiai informuoti apie stebimas vietas.	
ASMENS DUOMENŲ PERDAVIMAS Į TREČIĄSIAS ŠALIS			
22.	Įmonei privalomos taisyklės (toliau – BCR)	Asmens duomenys gali būti perduodami BCR pagrindu tik tuo atveju, jei asmens duomenys perduodami įmonių grupės viduje, kai dalis įmonių grupei priklausančių įmonių yra trečiojoje valstybėje.	
23.	Standartinės sutarčių sąlygos	Asmens duomenys gali būti perduodami į trečiąsias šalis, vadovaujantis standartinėmis duomenų apsaugos sąlygomis.	
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI IR SAUGUMO INCIDENTAI			
24.	Reagavimo į asmens duomenų saugumo pažeidimus tvarka	Tvarka turi nustatyti tinkamas procedūras, kaip aptikti, pranešti ir ištirti asmens duomenų saugumo pažeidimus. Tuo atveju, kai dėl pažeidimo dydžio bei svarbos gali kilti pavojus duomenų subjekto teisėms ir laisvėms, įmonė privalo nedelsdama pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą.	
25.	Pranešimo apie duomenų pažeidimą duomenų subjektui forma	Asmens duomenų pažeidimo atveju, dėl kurio gali kilti „didelė rizika asmens teisėms ir laisvėms“, turite užpildyti duomenų subjektų pranešimo apie duomenų pažeidimus formą.	
26.	Pranešimo apie duomenų pažeidimą priežiūros institucijai forma	Asmens duomenų saugumo pažeidimo atveju, apie kurį reikia informuoti VDAI, turite užpildyti duomenų pažeidimo pranešimo formą.	
27.	Asmens duomenų saugumo pažeidimų registras	Duomenų valdytojas privalo dokumentuoti visus asmens duomenų saugumo pažeidimus, įskaitant su asmens duomenų saugumo pažeidimu susijusius faktus, jo poveikį bei taisomuosius veiksmus. Remdamasi tais dokumentais, VDAI turi galėti patikrinti, ar laikomasi visų numatytų reikalavimų.	
TIESIOGINĖ RINKODARA			
28.	Sutikimo forma dėl tiesioginės rinkodaros naudojimo	Tiesioginė rinkodara gali būti vykdoma tik turint išankstinį duomenų subjektų sutikimą, išskyrus pagal įstatymą numatytais išimčių atvejais.	
29.	Teisės prieštarauti dėl tiesioginės rinkodaros pranešimų siuntimo įgyvendinimas	Asmuo, kuris teikdamas paslaugas ar parduodamas prekes gauna iš savo klientų elektroninio pašto kontaktinius duomenis, gali naudoti juos savo prekių ar paslaugų rinkodarai, jei klientams yra suteikiama aiški, nemokama ir lengvai įgyvendinama galimybė nesutikti arba atsisakyti tokio kontaktinių duomenų naudojimo.	
30.	Teisėto intereso vertinimo testas dėl tiesioginės rinkodaros	Tuo atveju, kai įmonė siunčia tiesioginės rinkodaros pranešimus, pasinaudodama įstatymo išimtimi, neturėdama duomenų subjekto sutikimo, ji privalo pagrįsti teisėtą interesą siųsti tiesioginės rinkodaros pranešimus. Organizacija turi įsitikinti, kad jos teisėti interesai nedaro didelio poveikio tų žmonių teisėms ir laisvėms.	
KITOS ORGANIZACINĖS DUOMENŲ SAUGUMO PRIEMONĖS			

31.	Asmens duomenų saugojimo politika	Šioje politikoje turėtų būti numatytas procesas, pagal kurį nusprendžiama, kiek laiko bus saugomi tam tikro tipo asmens duomenys bei kaip jie bus saugiai sunaikinti.	
32.	IT išteklių registras	Įmonė turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą. Tinkamas techninės, programinės bei tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui, nes tai leidžia kontroliuoti duomenų tvarkymo priemones. Išteklių valdymas būtinai turi apimti IT išteklių ir tinklo topologijos (schemos), kuri yra naudojama tvarkant asmens duomenis, registravimą.	
33.	Veiklos tęstinumo planas	Įstaiga turi nustatyti pagrindines procedūras, kurių turi būti laikomasi saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas tinkamas asmens duomenų tvarkymo IT sistemomis tęstinumas.	
34.	Veiklos įrašai	Dokumentas, kuriame fiksuojama įstaigos vykdomų duomenų tvarkymo veiklų tikslai, duomenų subjektai bei gavėjai, duomenų ištrynimo terminai ir kita reikalaujama ir reikšminga informacija apie duomenų tvarkymo veiklas.	
35.	Prieigos valdymo politika	Saugumo politika nustato pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus. Tai yra visų techninių ir organizacinių duomenų saugumo priemonių įgyvendinimo pagrindas. Remiantis šia politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose (pvz., įrenginių valdymo, išteklių valdymo). Saugumo politika, kurioje privaloma aiškiai išskirti asmens duomenų apsaugą, nustato bendrą organizacijos informacijos saugos valdymą.	
REKOMENDUOTINI TURĖTI DOKUMENTAI			
36.	Privatumo politikų registras	Šis dokumentas gali būti naudingas, jei privatumo pranešimai yra paskelbti daugelyje vietų ir norima kontroliuoti juos bei, jei yra poreikis, įsivertinti, kada ir koks pakeitimas buvo atliktas.	
37.	Poveikio duomenų apsaugai vertinimo tvarka	Dokumentas gali būti naudojamas atliekant poveikio duomenų apsaugai vertinimą.	
38.	Teisėto intereso vertinimo atlikimo tvarka	Itin naudingas dokumentas, atliekant teisėto intereso vertinimo testą.	
39.	Duomenų tvarkytojo atitikties klausimynas	Dokumentas gali būti naudojamas atliekant duomenų tvarkytojo atitikties BDAR reikalavimams patikrinimą.	
40.	Sutikimo atšaukimo forma	Naudingas dokumentas, jei duomenų subjektas norėtų atšaukti savo sutikimą dėl duomenų tvarkymo ir valdymo.	
41.	Tėvų sutikimo atšaukimo forma	Naudingas dokumentas, jei tvarkomi jaunesnių nei 14 metų asmenų duomenis.	
42.	Tarpvalstybinio asmens duomenų perdavimo tvarka	Naudingas dokumentas, jei asmens duomenis yra perduodami už Europos ekonominės erdvės ribų.	

Sąrašas parengtas pagal Bendrojo duomenų apsaugos reglamento (BDAR) nustatytus reikalavimus bei Valstybinės duomenų apsaugos inspekcijos (VDAI), Europos duomenų apsaugos valdybos (EDAV) ir 29 straipsnio duomenų apsaugos darbo grupės parengtas rekomendacijas, gaires ir nuomones.