

PERSONALISTO IŠŠŪKIAI **ASMENS** **DUOMENŲ** TVARKYMO SRITYJE

Miglė Petkevičienė

Ellex Valiūnas advokatų kontoros partnerė
Personalo valdymo profesionalų asociacijos atstovė

2023 m. sausio 30 d.

Šiandien kalbėsime

Didžiausi iššūkiai:

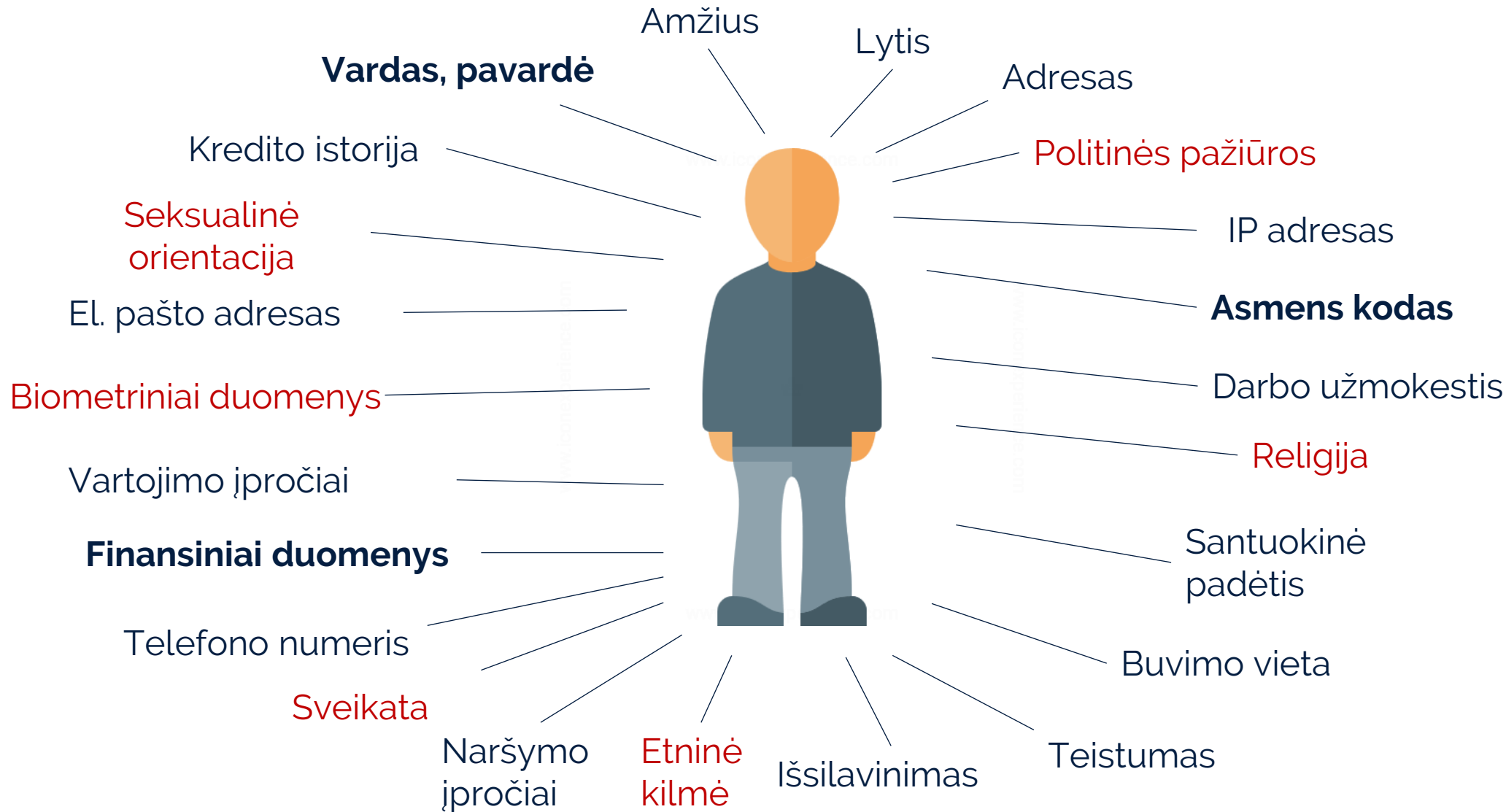
1. Suprasti, kiek ir kokius duomenis tvarko organizacija personalo srityje
2. „Būti viename puslapyje“ su kitomis organizacijos funkcijomis
3. „Įvaldyti“ reglamentavimo detalumą ir duomenų apsaugos specifiką
 - A. Kandidatai
 - B. Darbuotojai (kitais pagrindais dirbantys asmenys?)
 - C. Buvę darbuotojai
4. Tinkamai reaguoti nutikus incidentui



PROBLEMA #1:


Suprasti, kiek ir kokius duomenis tvarko organizacija personalo srityje

Asmens duomenys v. specialiuju kategoriju asmens duomenys



Asmens duomenų **personalo srityje** gausa



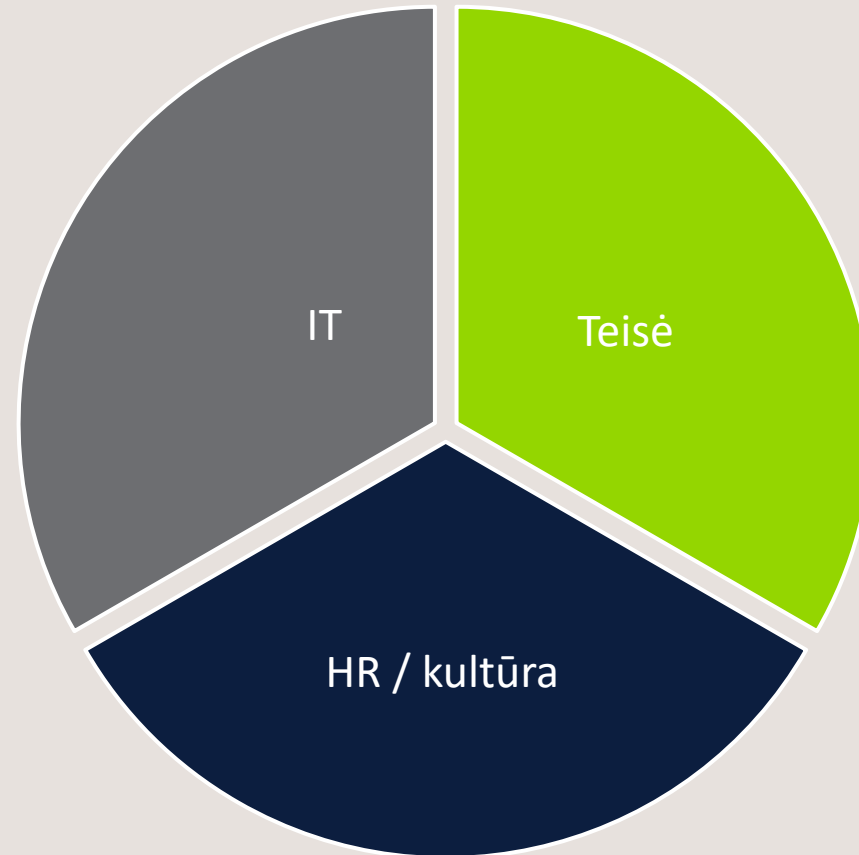


PROBLEMA #2:
„Būti vienam puslapyje“ su kitomis
organizacijos funkcijomis



Bendradarbiavimas ir komunikacija

3 esminieji „ingredienti“



Prioritetų nustatymas



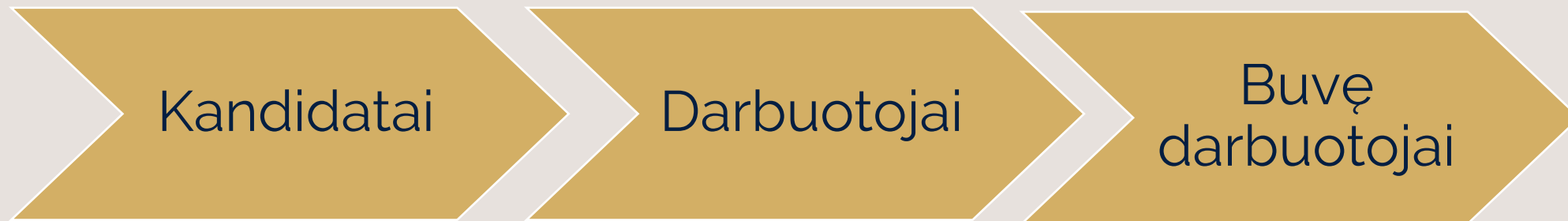


PROBLEMA #3:
„Įvaldyti“ reglamentavimo detalumą ir
duomenų apsaugos specifiką

Esminiai principai: jų veikimo pavyzdžiai



Darbuotojų asmens duomenų tvarkymas



- Informacijos rinkimas
- Tolesnis CV naudojimas

- Sutikimas kaip duomenų tvarkymo pagrindas (?)
- Stebėjimas

- Duomenų saugojimas
- Kontaktai ir tolesnis bendravimas



Kandidatų asmens duomenų tvarkymas

Galima rinkti	Negalima rinkti
vardas, pavardė 	šeiminė padėtis 
kontaktai  	duomenys apie tautybę 
adresas 	teistumas 
išsilavinimas 	duomenys apie administracines nuobaudas 
kvalifikacija 	artimų asmenų darbovietės 
gebėjimai 	duomenys apie narkotinių medžiagų vartojimą ir rūkymą  
Rekomendacijos / atsiliepimai:	asmens kodas 
iš esamo darbdavio – tik su sutikimu	asmeninis kredito reitingas 
iš buvusio darbdavio - informavus	

Bendra taisyklė: rinkti tiek duomenų kiek **būtina** (proporcingumas).

Darbuotojų stebėjimas



Automobilio judėjimo trajektorija **yra asmens duomenys**



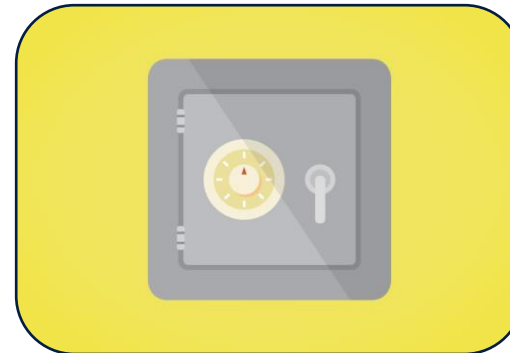
Privaloma **informuoti** darbuotojus



Rekomenduojama vietos stebėjimo programinę įrangą įrašyti **darbiniame** telefone, o ne asmeniniame



Būtina **aprašyti** vidiniame dokumente



Perduodami tik tuo atveju, jei užtikrinama **pakankamo lygio** apsauga



PROBLEMA #4:
Tinkamai reaguoti nutikus incidentui

Pranešimas apie pažeidimą



Kas yra duomenų saugumo pažeidimas?



Pranešimas:

- Pažeidimo pobūdis ir apimtis
- Kontaktai
- Tikėtinos pasekmės
- Priemonės, kurių imtasi
- Vėlavimo priežastys (jei po 72h)



Pranešimas inspekcijai vs. Pranešimas subjektams



Rekomendacija: šifravimas, darbuotojų apmokymas, procedūra

72 valandos



KAD SU IŠŠŪKIAIS TVARKYTIS BŪTŲ LENGVIAU:
namų darbai

Duomenų analizė (I)

Tikslas (-ai), kuriuo (-iais) tvarkomi asmens duomenys, pvz., priežastys, dėl kurių jie renkami, kodėl jie saugomi?

Asmens duomenų **šaltinis** – ar jie gauti iš paties asmens, ar iš kur nors kitur?

Kaip jie **naudojami** praktiškai ir ar tai atitinka nurodytą tikslą, dėl kurio jie iš pradžių buvo surinkti?

Tinkamų ir teisėtų **duomenų tvarkymo pagrindų** įsivertinimas.

Teisėti pagrindai tvarkyti bet kurios **specialios kategorijos asmens duomenis**. Šios kategorijos asmens duomenų tvarkymui taikomos papildomos, siauresnės taisyklės.

Duomenų analizė (II)

Asmens duomenų **buvimo vieta**, pvz., ar jie saugomi paties darbdavio sistemoje, ar išorinėje trečiosios šalies sistemoje, ar yra vienoje, ar keliose vietose, o jei pastarojoje, ar toks dubliavimas yra būtinas?

Asmenys (vidaus ir išorės) ir organizacijos, kurie turi **prieigą** prie asmens duomenų (pvz., tiesioginiai vadovai, žmogiškųjų išteklių personalas, administracija arba paslaugų tiekėjai). Ar šių asmenų prieiga praktiškai yra būtina?

Kur asmens duomenys yra **perduodami** tiek viduje, tiek išorėje (įskaitant bet kokį tarptautinį duomenų perdavimą), pvz., išmokų tiekėjams?

Kokios **saugumo priemonės** yra taikomos saugant, tvarkant ir perduodant asmens duomenis, kad jie būtų saugūs?

Duomenų analizė (III)

Jei asmens duomenys perduodami už EEE ribų, **kokie mechanizmai yra taikomi**, užtikrinant perduodamų duomenų saugumą ir atitiktį BDAR standartams?



Kokios yra taikomos asmens **duomenų saugojimo ir ištrynimo priemonės**? Kiek laiko yra saugomi asmens duomenys, ar galima pagrįsti tokį ar kitokį saugojimo laikotarpį ir koku pagrindu?



Ar vykdant žmogiškųjų išteklių procesus priimami **automatizuoti sprendimai**, pvz., įdarbinant (automatinis atmetimas ir atranka) arba nustatant neatvykimo į darbą priežastis?

Dokumentacijos veiksmų planas

Parengti arba atnaujinti **duomenų saugojimo politiką**, kurioje turėtų atsispindėti organizacijos požiūris į duomenų saugojimą, saugojimo priešastys, pagrindai (**vengti sutikimo!**), kriterijai, kuriais remiantis nustatomas saugojimo laikotarpis (jei neįmanoma nurodyti tikslaus termino).

Parengti **duomenų saugumo pažeidimų politiką**, jei ji nėra įtraukta į platesnę duomenų apsaugos politiką.

Parengti arba atnaujinti **pranešimus apie duomenų privatumą**, kad juose būtų pateikta informacija, kurią pagal BDAR reikalaujama pateikti duomenų subjektams. Be kita ko tai apima – duomenų tvarkymo tikslą, teisinius pagrindus, asmenų prieigą prie duomenų (tiek viduje, tiek išorėje).

Parengti arba atnaujinti **duomenų apsaugos politiką**, kurioje turėtų būti nurodyta kaip organizacija laikosi duomenų apsaugos reikalavimų, koks procesas taikomas duomenų saugumo pažeidimų atvejais.

Nustatyti, kokių duomenų apsaugos nuostatų pakeitimų reikia **darbo sutartyse ir kituose sutartiniuose dokumentuose**.

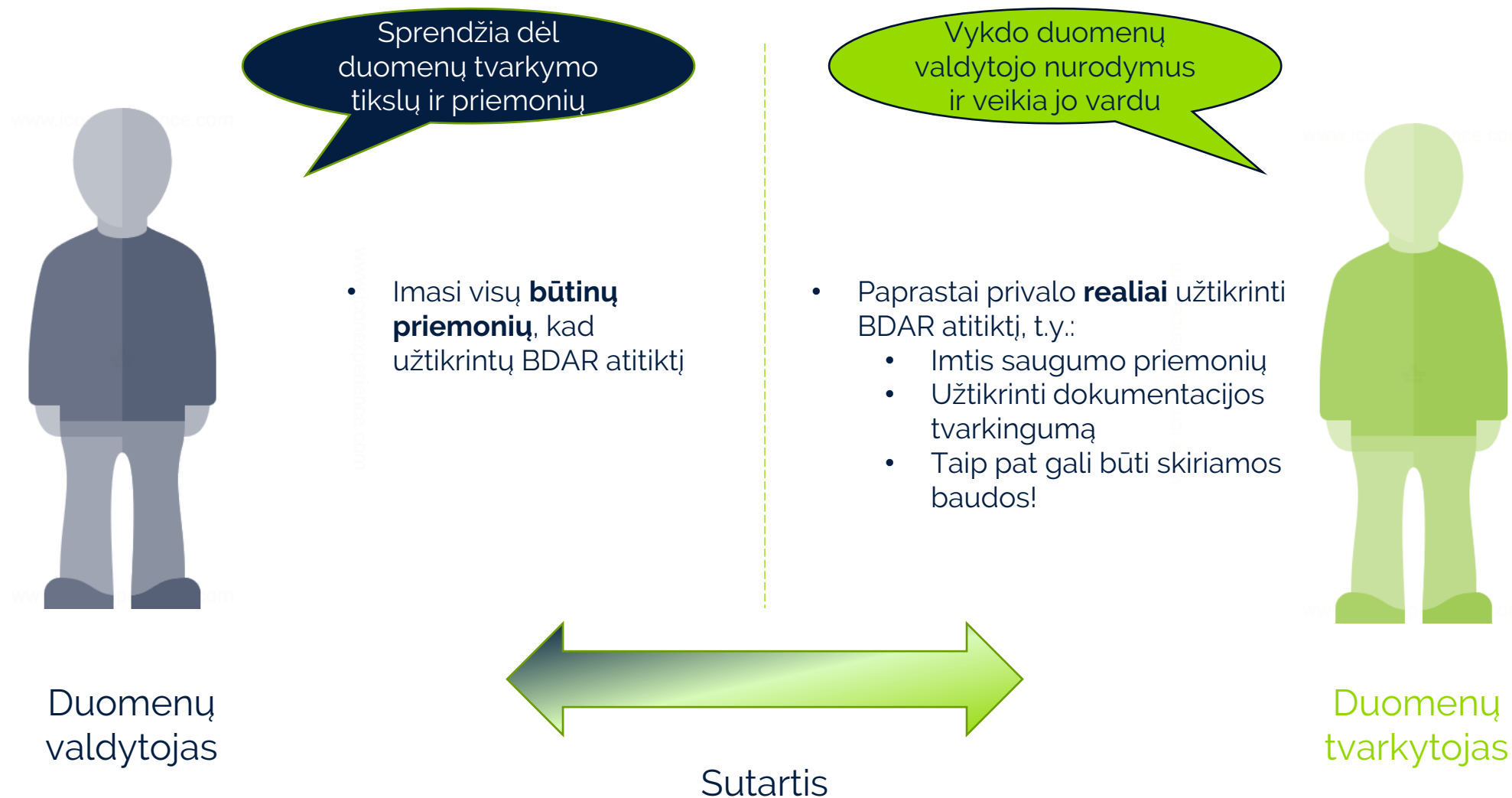
Asmens duomenų perdavimas ir duomenų tvarkytojų dalyvavimas

Jei asmens duomenys perduodami **duomenų tvarkytojams**, patikrinkite, ar organizacijos susitarimai su jais atitinka BDAR reikalavimus, įskaitant privalomus sutartinius įsipareigojimus.

Jei asmens duomenys perduodami **trečiosioms šalims**, patikrinkite, ar tam yra teisėtas pagrindas ir ar yra mechanizmai, skirti informuoti trečiąsias šalis apie bet kokius veiksmus, kurių imamasi pasinaudojus duomenų subjekto teisėmis, pvz., prašymu ištaisyti netikslią informaciją arba apriboti duomenų tvarkymą.

Jei asmens duomenys turi būti perduodami **už EEE ribų**, patikrinkite, ar taikomi tinkami ir saugūs mechanizmai, užtikrinantys duomenų saugumą, ir ar duomenų perdavimo pagrindas atitinka būtiniausius BDAR standartus.

Duomenų valdytojas v. duomenų tvarkytojas



Kiti atliktini veiksmai

Duomenų saugojimas

- Užtikrinti, kad būtų įdiegtos sistemos, leidžiančios ištrinti asmens duomenis pagal saugojimo politiką arba tam tikrais atvejais atlikti anonimizavimą, užtikrinant, kad tai būtų atlikta saugiai.
- Ištrinti pasenusius duomenis, kurių saugojimo laikotarpis viršijo atitinkamą laikotarpį. Duomenų kiekio mažinimas yra vienas pagrindinių BDAR principų.

Duomenų subjektų teisių užtikrinimas

- Užtikrinkite, kad būtų įdiegti tinkami procesai, skirti duomenų subjektų teisėms įgyvendinti. Tai apims prieigos prie duomenų subjektų prašymų politikos ir šabloninių laiškų, kuriais atsakoma į prašymus, parengimą arba atnaujinimą.
- Jei sprendimai priimami automatizuotai, patikrinkite, ar tam yra teisėtas pagrindas ir ar taikomi atitinkami mechanizmai, kad asmuo galėtų užginčyti sprendimą.

Duomenų saugumas ir jo pažeidimai

- Pašalinkite visas nustatytas informacijos saugojimo saugumo spragas ir apsvarstykite, ar reikia atlikti pakeitimus, pvz., apsaugoti sistemos failus slaptažodžiu arba apriboti prieigą prie elektroninių failų.
- Užtikrinkite, kad būtų įdiegti procesai, skirti duomenų privatumo pažeidimams pašalinti ir apie juos pranešti per BDAR nustatytus trumpus terminus.

Mokymai ir informuotumas

- Mokykite visus organizacijos darbuotojus, kurie tvarko asmens duomenis, ir užtikrinkite, kad jie būtų susipažinę su galiojančia ar peržiūrėta politika.
- Užtikrinkite, kad darbuotojai būtų informuoti apie politikos ir procesų pakeitimus.

Ellex[®]



Ačiū!



Miglė Petkevičienė

Partnerė

T: +370 640 41055

E: migle.petkeviciene@ellex.legal