



PRIVACY
PARTNERS

PRIVACY • CARE • SECURITY • COMPLIANCE
WWW.PRIVACYPARTNERS.LT

Kaunas, 2018 12 05
Klaipėda, 2018 12 06

Martynas Bieliūnas, CIPP / E
Vykdantysis partneris
Martynas@privacypartners.lt



VERSLO IR ASMENS DUOMENŲ APSAUGA:

KAIP SUSTIPRINTI ĮMONĖS KONKURENCINGUMĄ?

Įvadas

Kodėl privatumas yra vienas iš esminių klausimų šiandienos organizacijoje – priežastys ir analizė



Teisė – BDAR

BDAR yra vienas iš esminių teisinių aktų, susijusių su privatumu. Pagrindiniai principai ir teiginiai, palyginimas



PRIVACY
PARTNERS

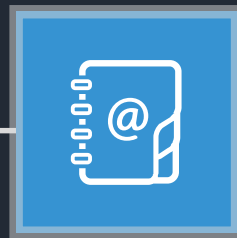
IT& Cloud BDAR'e

Kaip susitvarkyti technologijas



Planas atitkčiai

Kokius principus ir teises reikia užtikrinti
Kokie asmens duomenys gali būti
Ką veikia duomenų apsaugos pareigūnas



Atitikties nauda

Ką įneša į įmonę sutvarkyta BDAR
atiktis



PRADŽIA

Jūsų organizacijos **privatumo ir BDAR atitikties** veikloms



PRIVACY
PARTNERS

ĮVADAS – BDAR PRIEŽASTYS

Asmens duomenys yra vienintelis būdas identifikuoti Jūsų klientą, partnerį, darbuotoją, interesantą

Asmens duomenų praradimas, tapatybės vagystės, manipuliacijos pasinaudojant socialine inžinerija liečia visas organizacijas

Situacijos analizė bei būdai kaip šalys ir vyriausybės atsako į šiuos iššūkius



Stambūs duomenų praradimai 2007-2018 m.

Šaltinis:

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



Globalios tendencijos

KONFLIKTUOJANČIOS VYSTYMOSI KRYPTYS



Atvirumas, sąveika, tarptautinis bendradarbiavimas, inovacija

Atviri duomenys, bendri standartai, globalios technologijos

VS.

Saugumas, izoliacija, nuosavybė, vystymas, stiprinimas

Privatumas, informacinė sauga, reguliavimas, ribojimas, tvarka

HIBRIDINĖS GRĖSMĖS

INTEGRUOTOS rizikos ir grėsmės

80%

didesnių incidentų turi savo „konstrukcijoje“ socialinės manipuliacijos komponentus

TECHNOLOGINĖS

IT grėsmės: virusai, Ransomware, keyloggers, DDoS atakos, kt.



SOCIALINĖS MANIPULIACIJOS

Fake news, Phishingas, web atakos

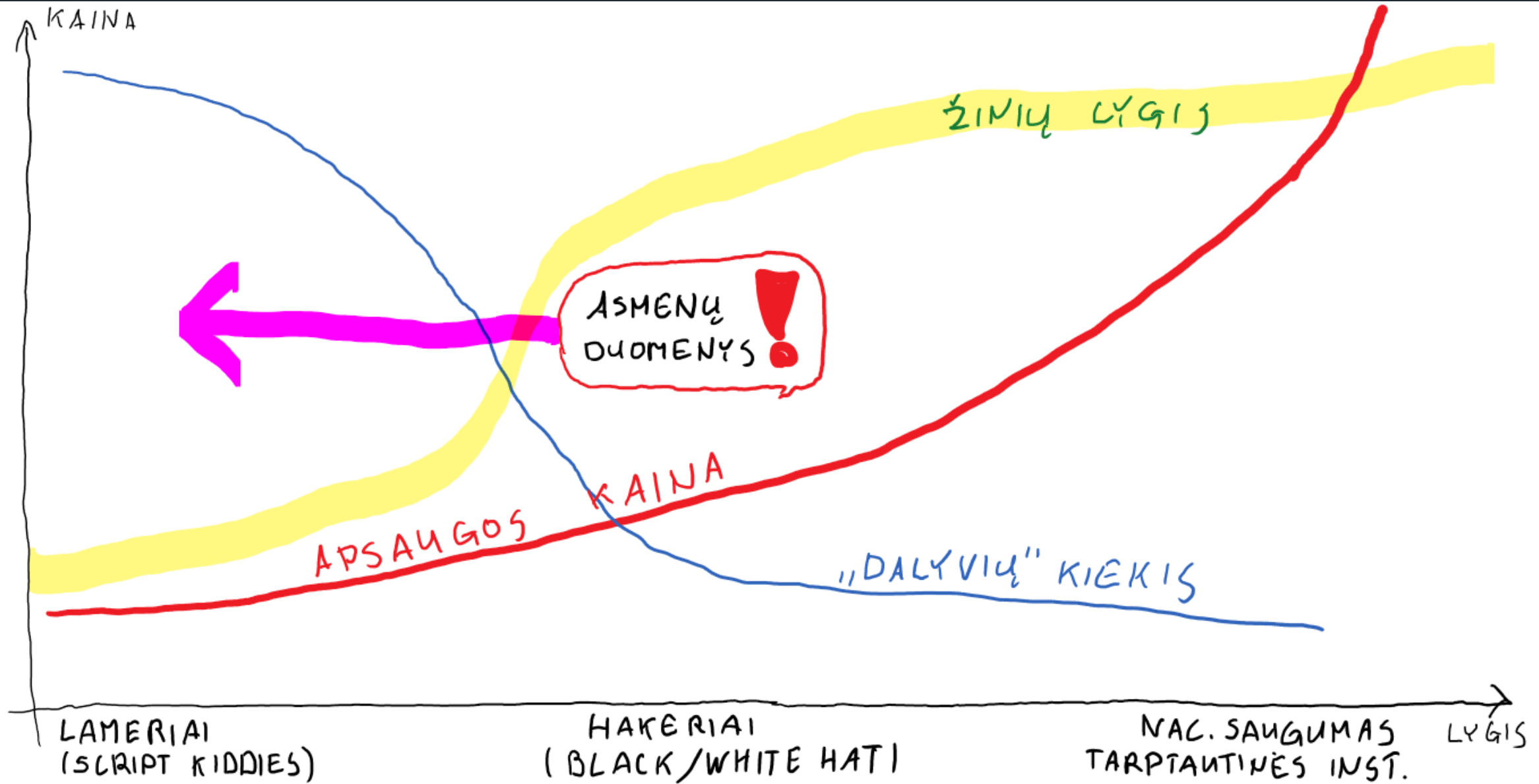


FIZINĖS GRĖSMĖS

Fizinės infrastruktūros problemos



ASMENS DUOMENYS KAIP NESANKCIONUOTŲ VEIKLŲ OBJEKTAS



KAS PASKATINO GRIEŽTESNĘ PRIVATUMO APSAUGĄ ?



Technologinis progresas

Duomenų rinkimas didėja tiek „į gylį“, tiek „į plotį“



Politinės priešpriešos

Nutrūkusios ES ir US sutartys, didėjančios izoliacionistinės tendencijos, skirtingos teisinės normos



Orientacija į klientą

Kokybiškai rinkodarai tinkla reikalingi didžiuliai asmens duomenų kiekiai. Jūs žinote apie klientą **daugiau** negu jis pats.



PRIVACY
PARTNERS

"In God we trust, others must bring data"
(Dievą tikime, o visi likę turi pateikti duomenis)



W. Edwards Deming

leading management thinker in the field of quality, 1900-1993



PRIVACY
PARTNERS

ASMENS DUOMENŲ VERTĖ IR REIKŠMINGUMAS



AUTENTIFIKACIJA

Nėra kitų būdų nustatyti asmenį iš kaštų ir patogumo perspektyvos



NĖRA ALTERNATYVŲ

Vartotojai de facto nelabai turi alternatyvų – be autentifikacijos jie negalėtų dalyvauti darbinėse, socialinėse ir kitose aplinkose. IT sistemos naudojamos be kontrolės kas vyksta su jų asmens duomenimis



SUTIKIMAI

Seniau kurtose sistemose asmens duomenys dažnai saugomi be aiškaus asmens sutikimo, tikslų ar teisėto pagrindo nurodymo.



KAINA & VERTĖ

Asmens duomenų vertę ir kainą labai sudėtinga apibrėžti objektyviai. Teisėje sudėtinga operuoti kategorijomis su verte “nuo 0 to ∞ ”



“RINKA”

Tuo pat metu asmens duomenys turi aiškią ir apibrėžtą kainą „juodoje rinkoje“ (dark web). Kartu su anoniminių atsiskaitymų priemonėmis, tai labai supaprastina prekybą vogtomis tapatybėmis ar finansiniais duomenimis.



ŠALTINIAI

Didejant technologijų skverbčiai, asmens duomenys renkami bet kur, dažnai vartotojui to net neįsąmoninant (mobilios tech., daiktų internetas, web tinklapiai, sekimas)



TEISINĖ BAZĖ: NE TIK EUROPA

Teisiniai klausimai į kuriuos reikia atsižvelgti valdant
PRIVATUMĄ



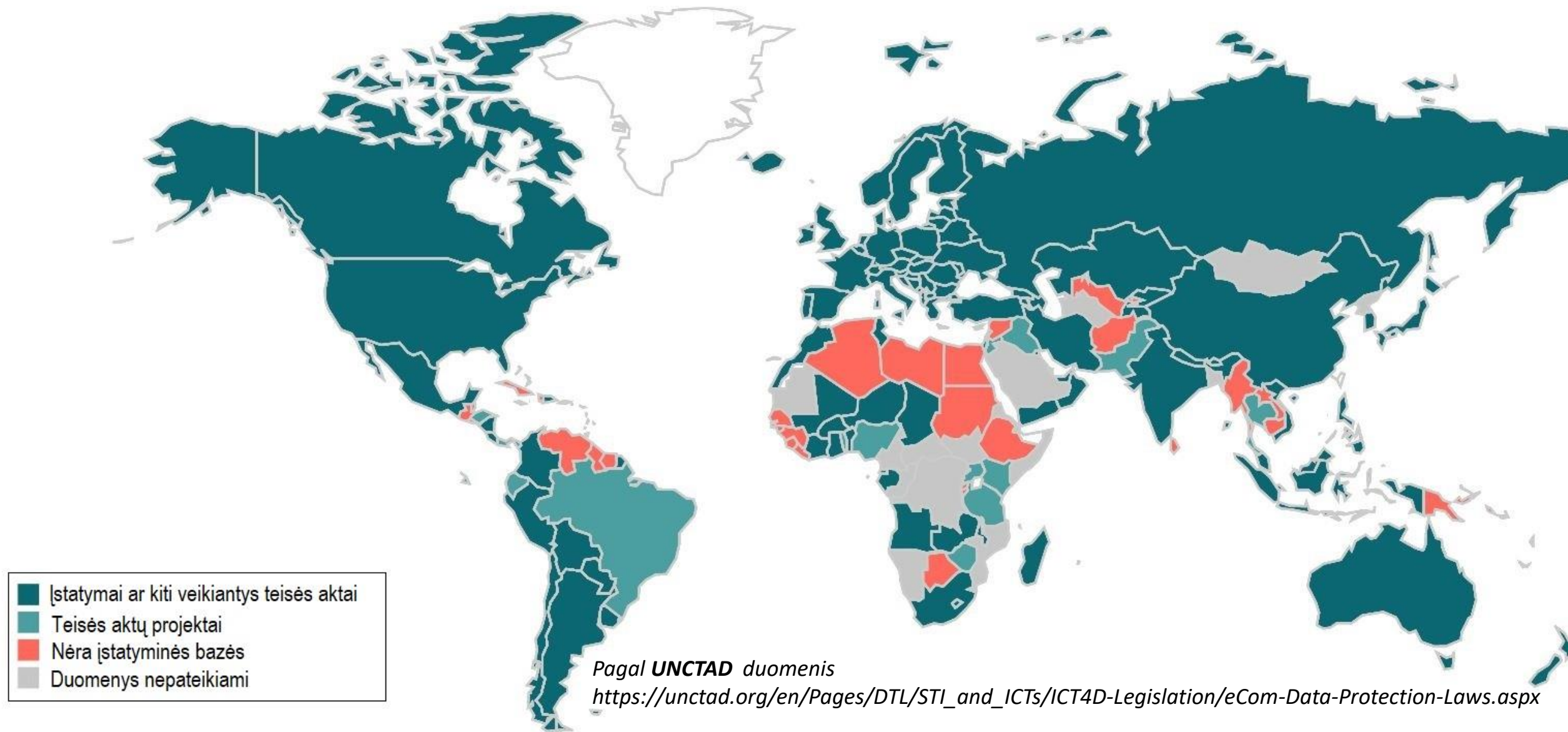
ASMENS DUOMENYS - TURTAS

Valstybės taip pat tai laiko savo ištekliais

- Piliečių saugumas ir privatumas
- Valstybės apsauga (bei kitų valstybių įtakojimas)
- Virtualių piliečių galimybė



ASMENS DUOMENŲ APSAUGOS ĮSTATYMAI



Globaliai apie 750 organizacijų kasdien priima apie 201 įstatyminių aktų susijusių su privatumu, pakeitimų (Microsoft)

BDAR PRINCIPAI





... Prieš rašydamas savo vardą ant lentos, turiu sužinoti kaip Jūs planuojate panaudoti šią informaciją

DUOMENŲ SUBJEKTO TEISĖS (III skyrius)

Visos organizacijos turi **įgyvendinti** duomenų subjekto teises jo sistemose ir procesuose



TEISĖ SUSIPAŽINTI

15 straipnis

Duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis



TEISĖ REIKALAUTI IŠTAISYTI DUOMENIS

16 straipnis

Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslius su juo susijusius asmens duomenis



TEISĖ „BŪTI PAMIRŠTAM“

17 straipnis

Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis



TEISĖ APRIBOTI DUOMENŲ TVARKYMĄ

18 straipsnis

Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų duomenų tvarkymą



TEISĖ Į DUOMENŲ PERKELIAMUMĄ

20 straipsnis

Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui



TEISĖ NESUTIKTI

21 straipnis

Duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi



VALDYTOJAS vs. TVARKYTOJAS

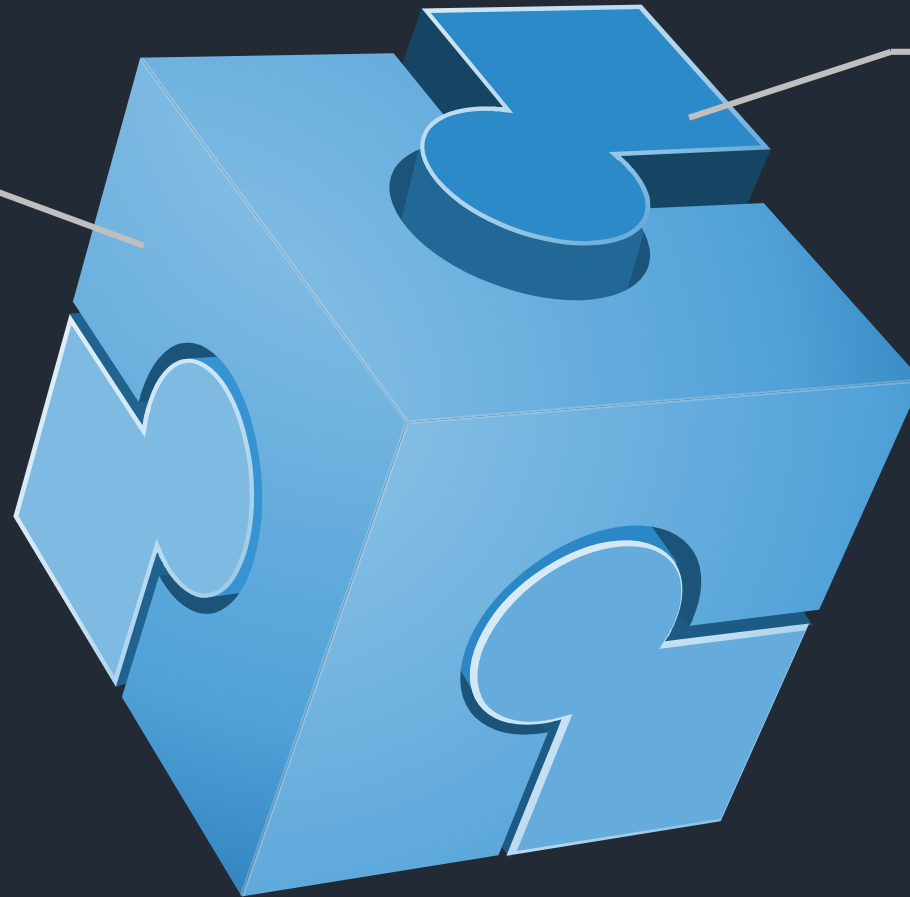
Duomenų valdytojai ir tvarkytojai (4 BDAR straipsnis)



Valdytojas

Nustato asmens duomenų
rinkimo ir naudojimo
tikslus ir priemones

Valdytojas yra atsakingas už
AD rinkimo tikslus IR už
tvarkytojų pasirinkimą



Tvarkytojas ☁

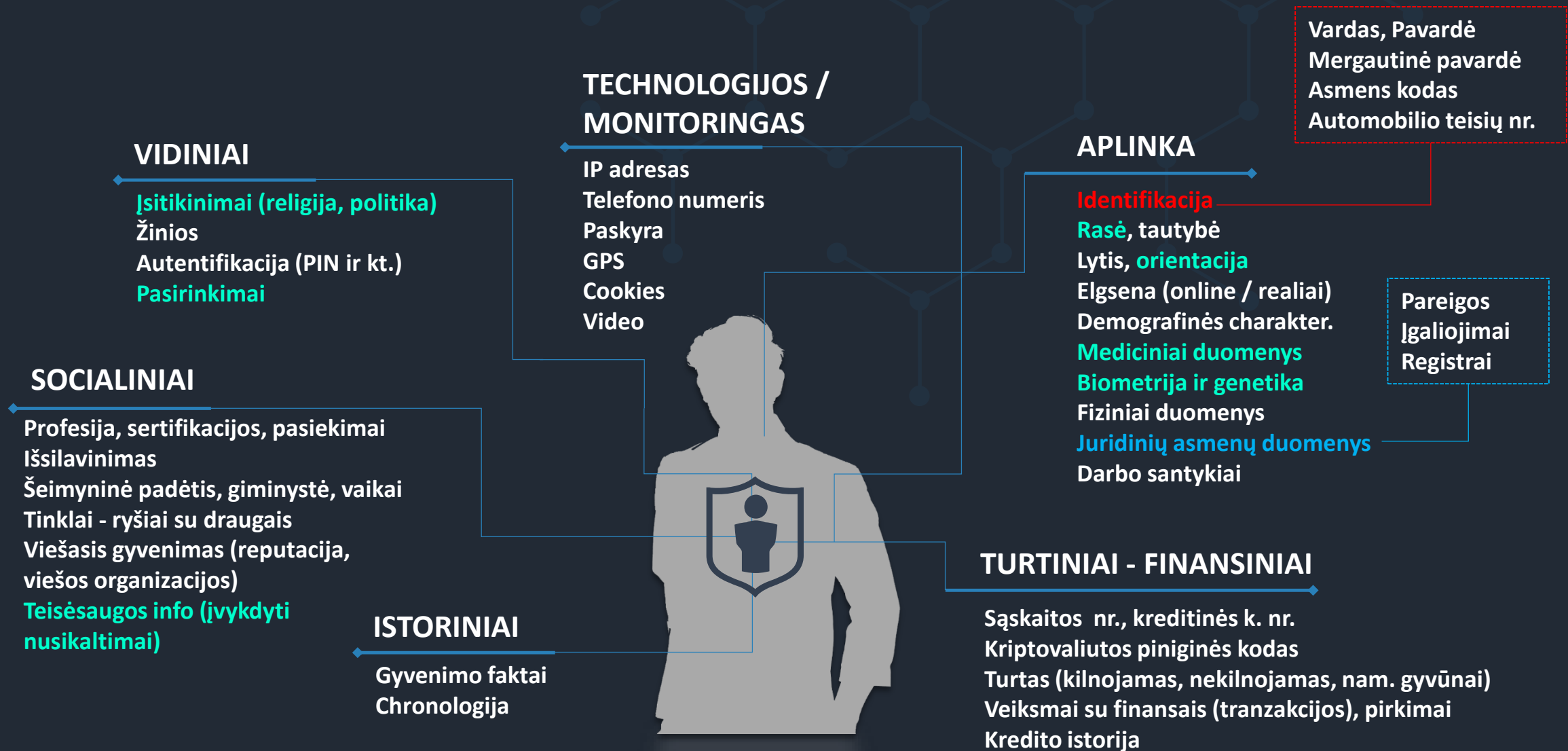
Tvarko asmens duomenis
valdytojo vardu

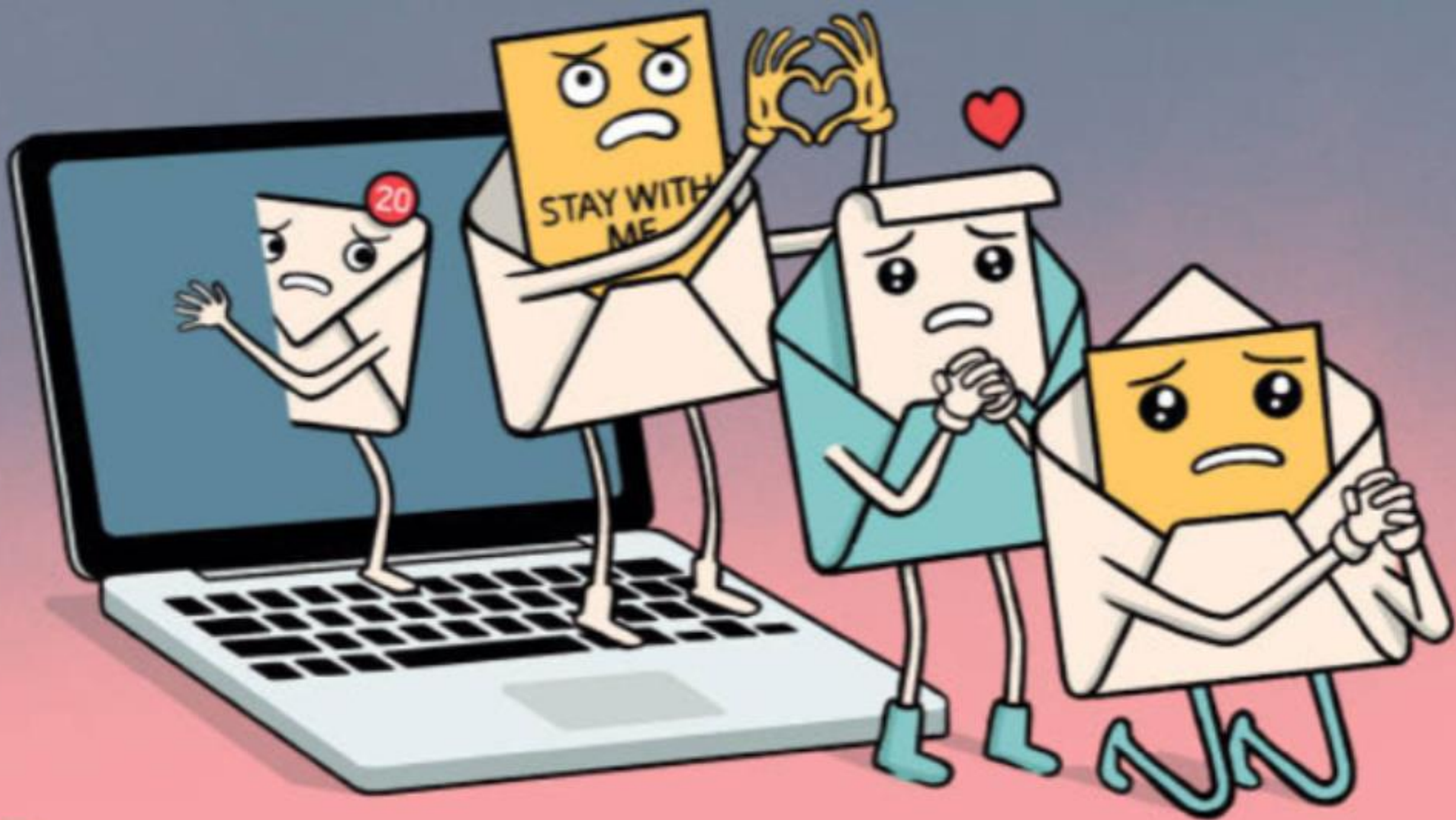
Jei tvarkytojas ima naudoti
asmens duomenis tikslams,
nesuderintiems su valdytoju,
jis automatiškai tampa
asmens duomenų valdytoju



PRIVACY
PARTNERS

Asmens duomenų kategorijos





Kliento sutikimas

Kaip **teisingai sudaryti** sutikimo formą asmens duomenų rinkimui



01

Faktai, terminai

Reikia įrodymo, kad sutikimas duotas bei kiek laiko galioja



02

Aiškumas

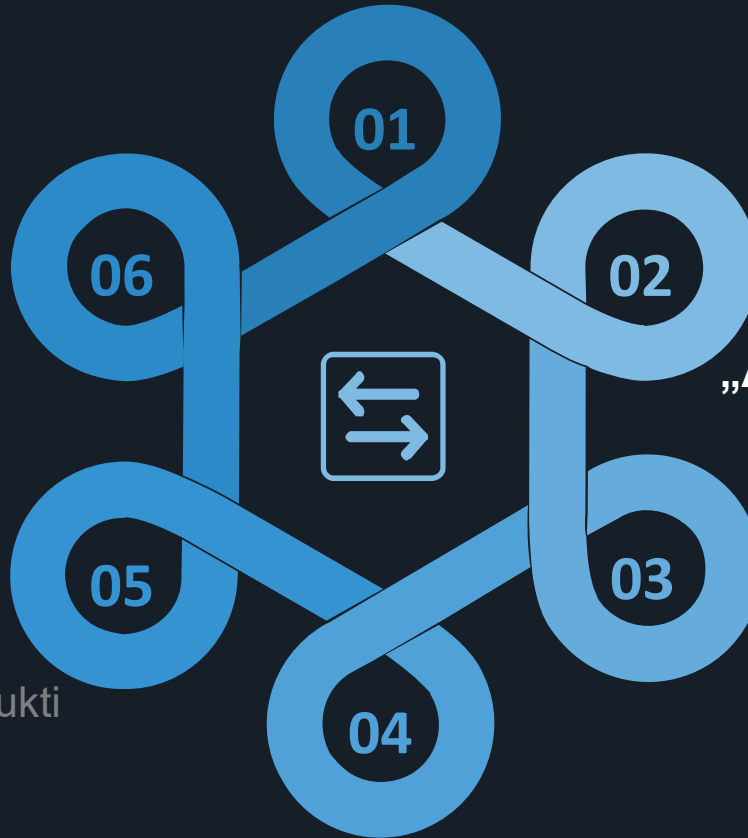
Atskiras nuo kitų klausimų, paprasta kalba



03

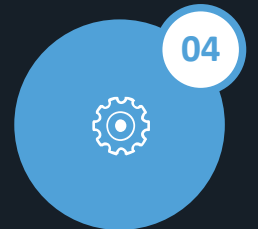
Atsisakymas

Galimybė bet kada atšaukti duotą sutikimą



Konkretūs tikslai

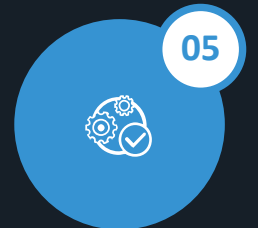
Negalima gauti bendrinių sutikimų, kuriuose nėra sukonkretinta AD rinkimo tikslai



04

„Automatiniai“ sutikimai

“by default”, “opt – out” sutikimai nebetinkami, reikia gauti sutikimą kiekvienai operacijai.



05

Teisingai gauti

Sutikimas netinkamas kai pozicijos nėra lygiavertės (pvz. darbdavys – darbuotojas). Tada naudojamas informavimas



06



Amžius

Vaikas negali duoti sutikimo (iki 16 m., gali kisti priklausomai nuo ES šalies. Minimalus amžius - 13 metų.)

Tipinis per ilgų sutikimų ir privatumo politikų pavyzdys
(atspausdintos Instagram, Facebook, Twitter, Snapchat
ir kitų soc. tinklų sutikimų ir privatumo politikų formos)



Iliustracija paimta iš: © Designer: Dima Yarovsky
Institution: Bezalel Academy for Art and Design
Jerusalem, Israel

ATITIKTIES PROJEKTAI

Į ką atsižvelgti tvarkant BDAR atitiktį
Verslo bei technologijų aspektai



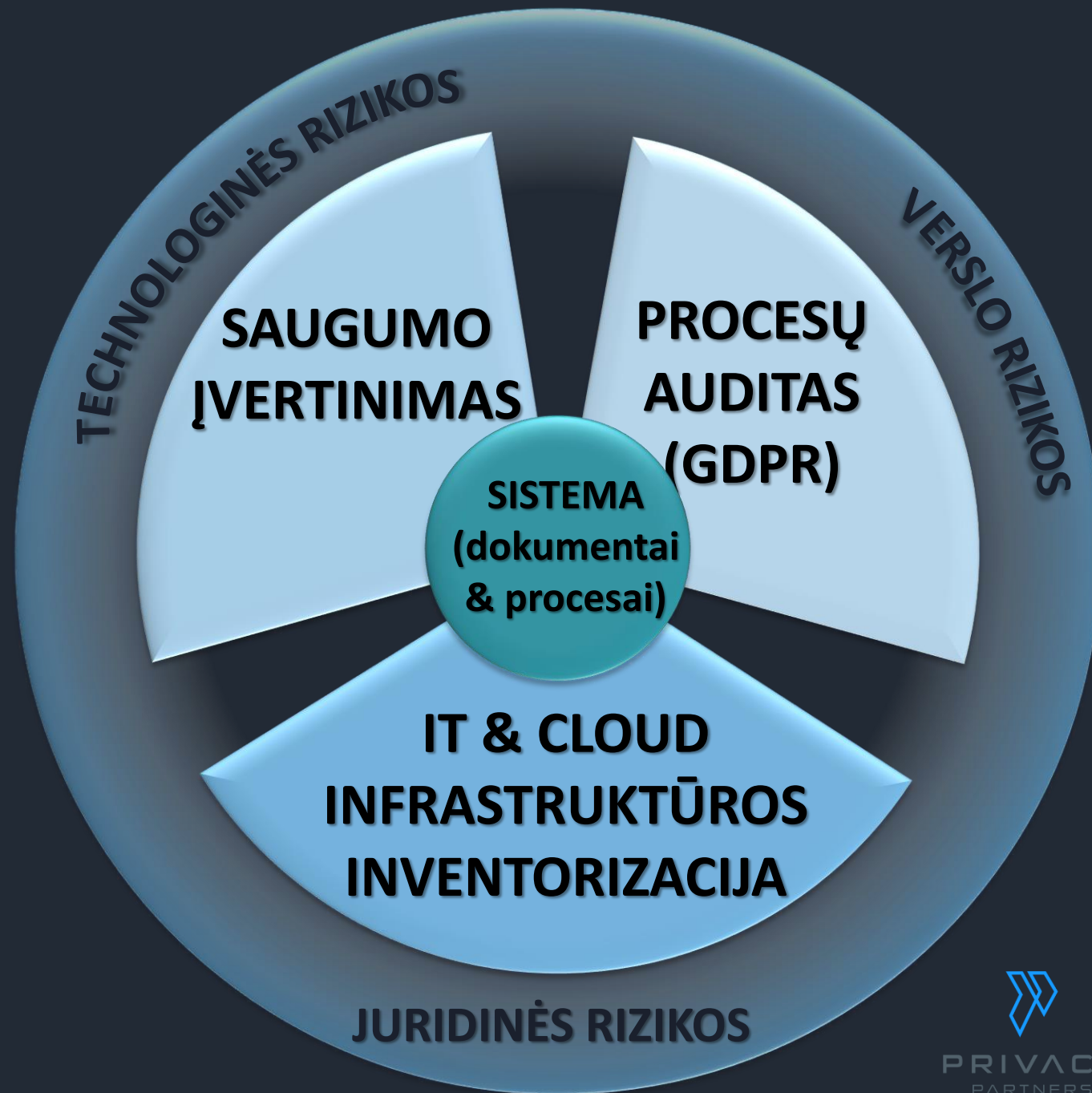


GDPR - BDAR

Visuose projektuose užtikriname aukštą technologijų, procesų ir teisinės dalies atitikties lygį.

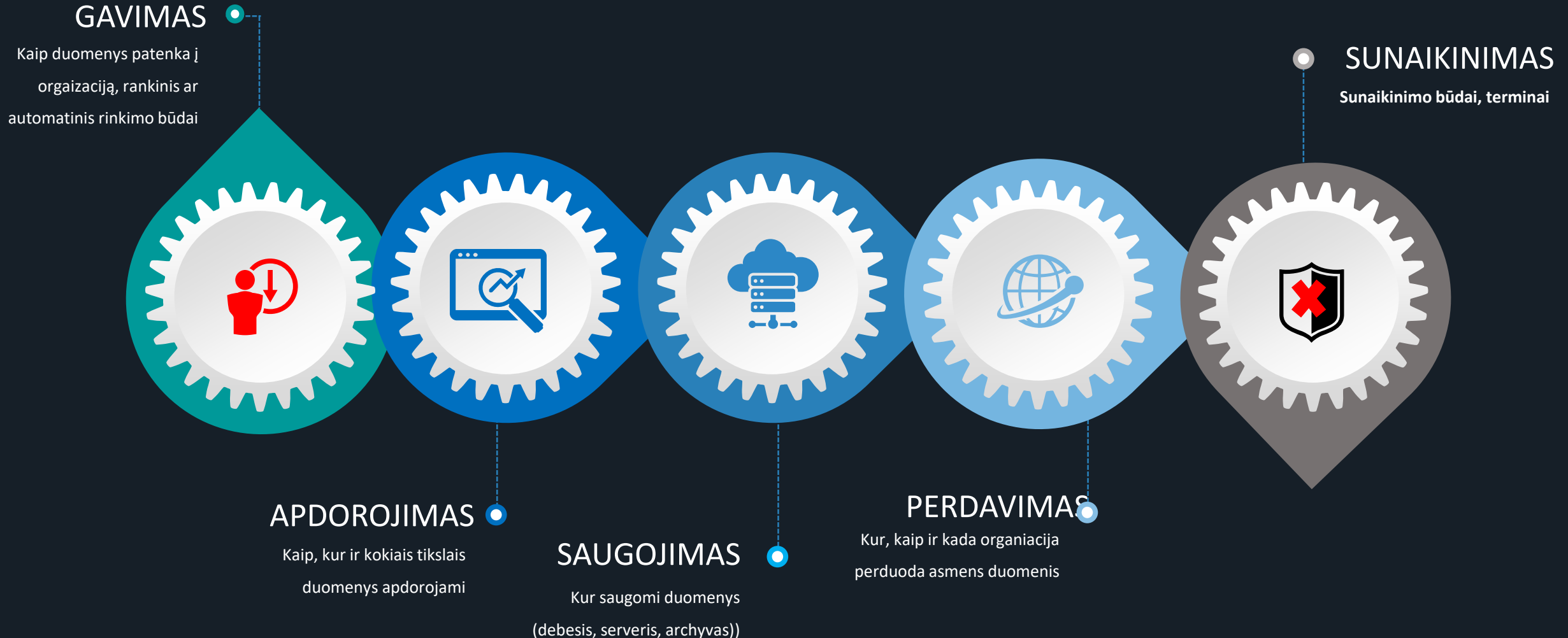
Atitiktis pasiekama tik įvertinus IT, realių verslo procesų ir teisinio reguliavimo visumą įmonėje bei pasvėrus galimas rizikas.

GDPR nėra vienkartinis procesas o reguliari sistemų, procesų ir teisinės dalies priežiūra.

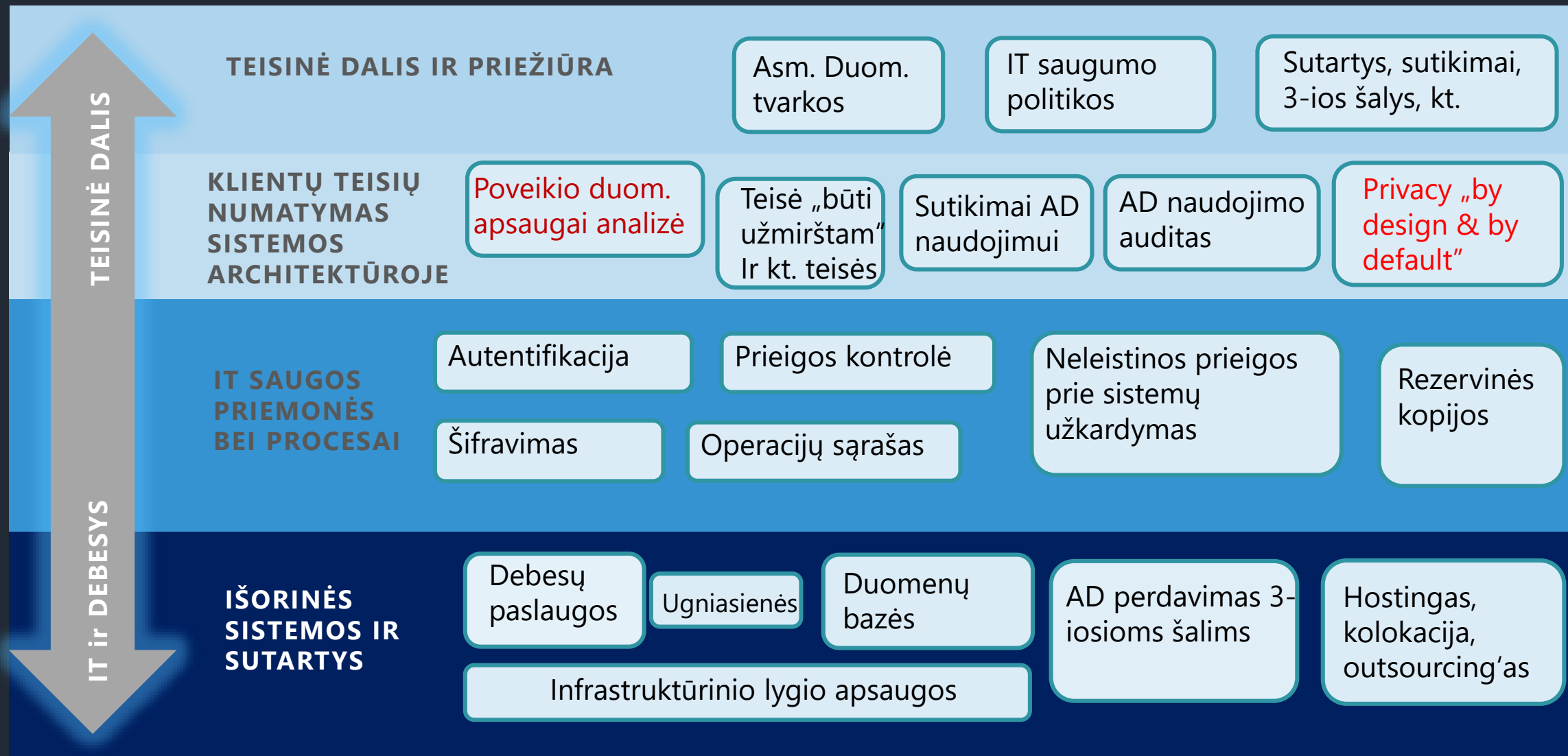


Asmeninių duomenų gyvavimo ciklas

Duomenų **procesų** supratimas



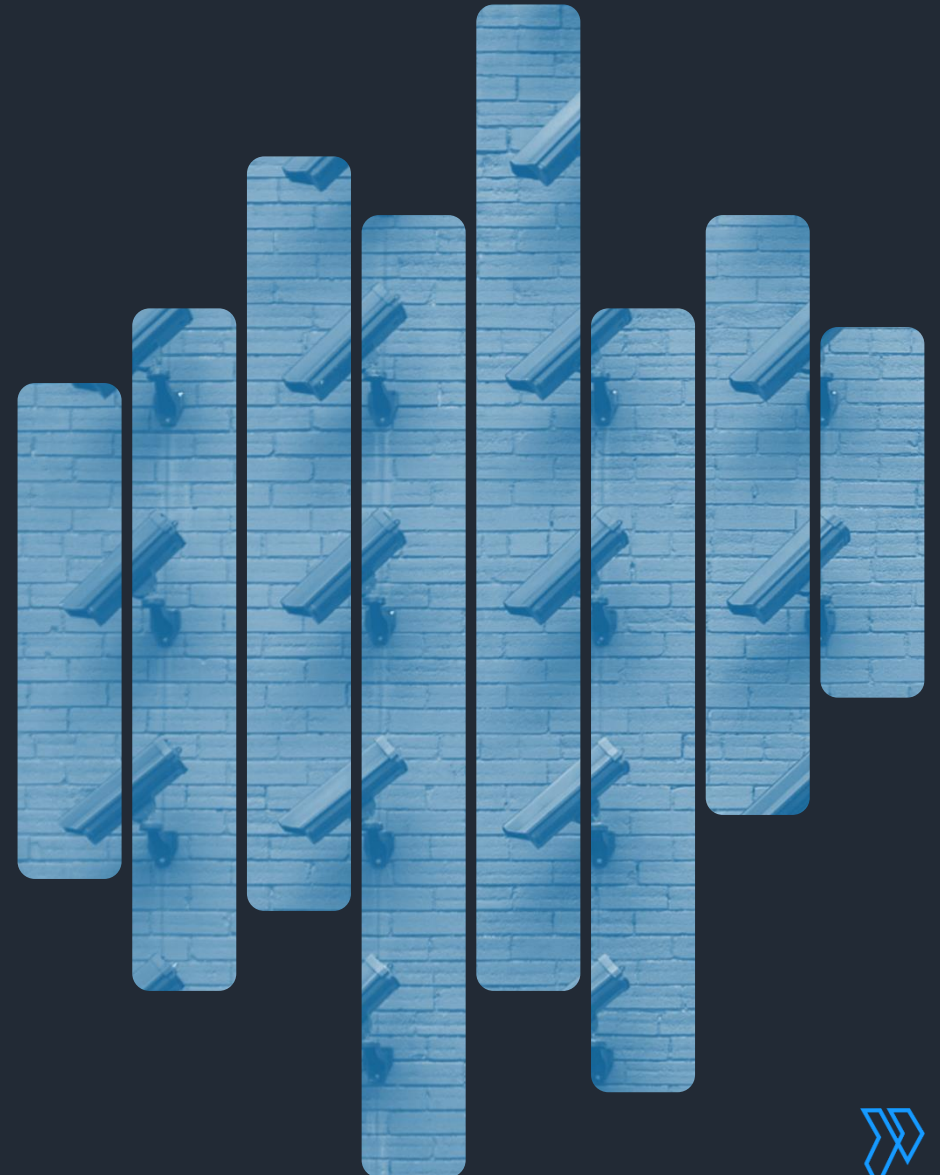
ASMENS DUOMENYS DEBESYJE IR IT



TECHNOLOGIJOS

(„Tipinės problemos“ randamos GDPR atitikties projektuose)

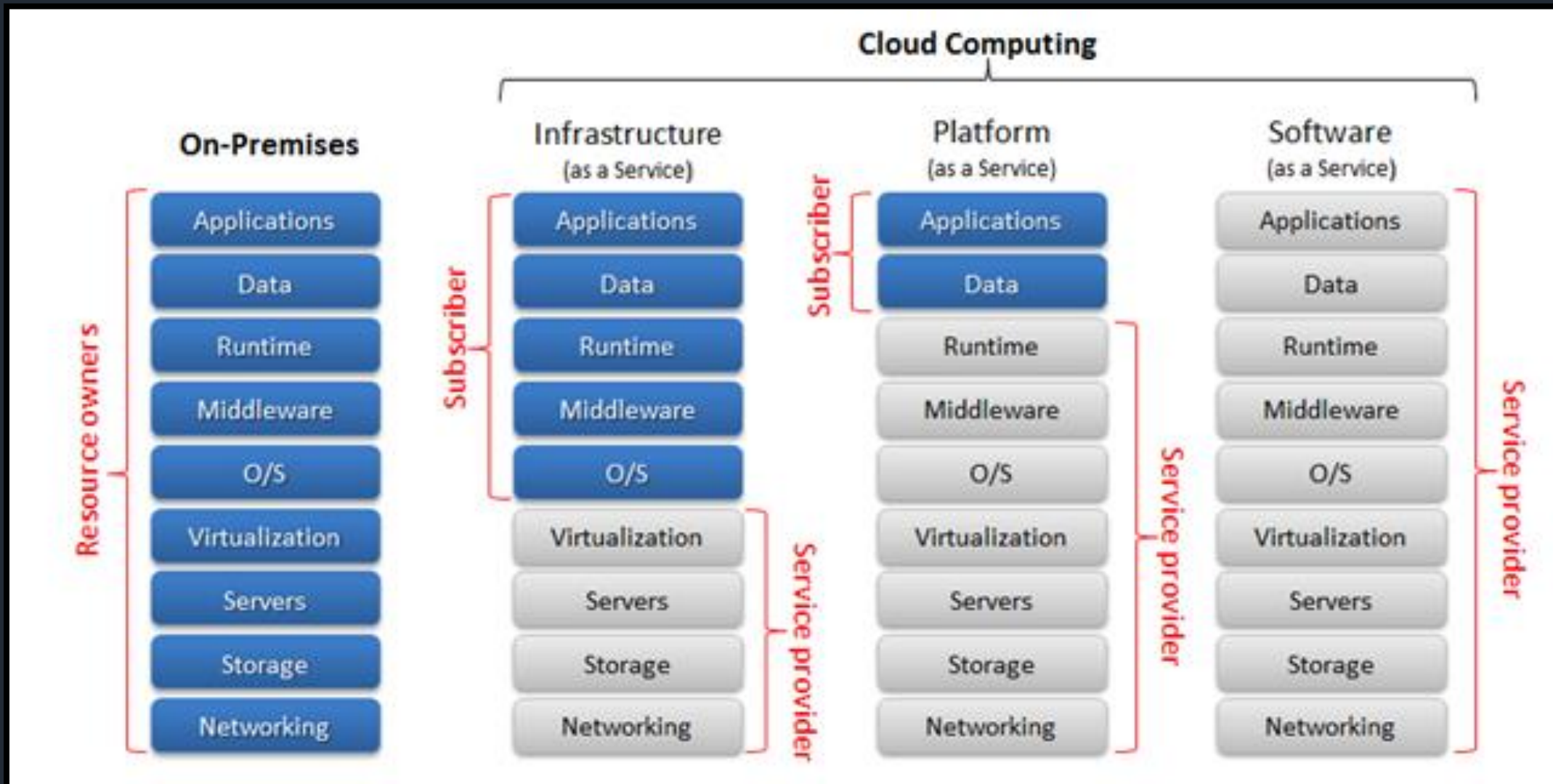
1. Šifravimas (duomenų);
2. Šifravimas (perduodant);
3. Klasifikacija;
4. Duomenų praradimo apsauga (Data loss prevention);
5. Pranešimai apie įsilaužimą (Data breach notification);
6. Slaptažodžių politika;
7. Prieigos kontrolė;
8. Duomenų srautų kontrolė;
9. Rezervinės kopijos;
10. Atnaujinimai, papildymai;
11. Operacijų log'ai, sekimas, auditas;
12. Ugniasienės problemos (Firewall / DMZ);
13. Antivirusai, apsauga nuo kenkėjiškos PĮ



PRIVACY
PARTNERS

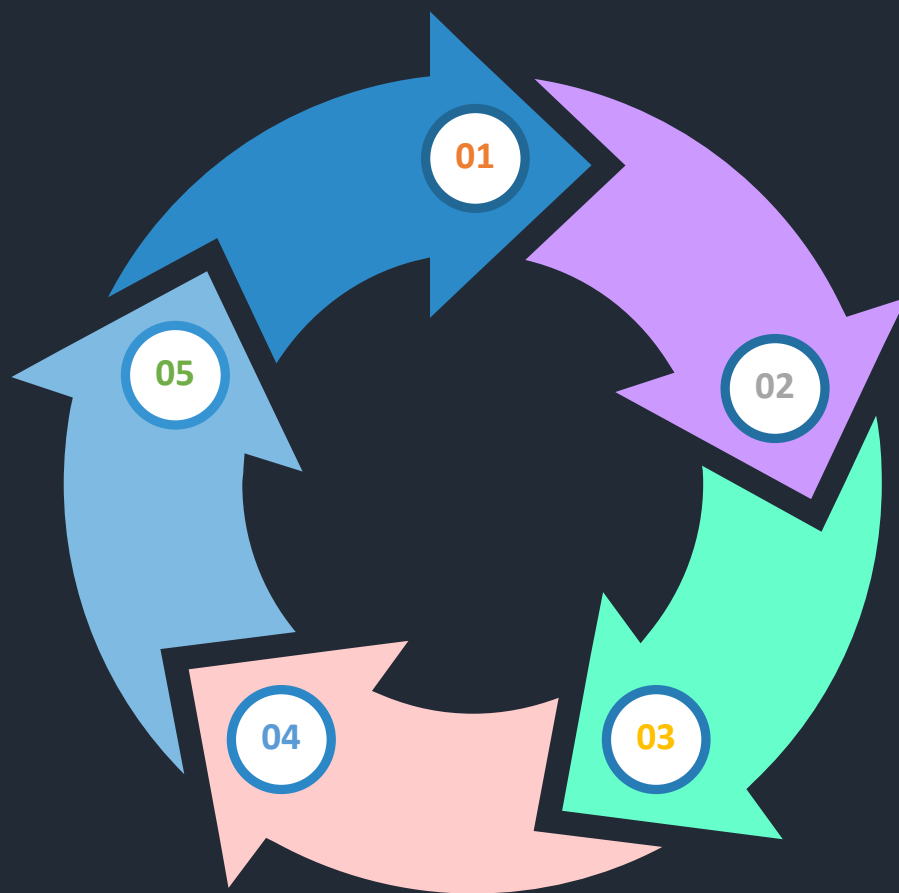
Jūs organizacija ar paslaugos tiekėjai?

ATSAKOMYBĖS PASIDALINIMAS:

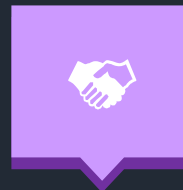


DAP veikla organizacijoje

Partnerystė ir priežiūra **visais** asmens duomenų klausimais



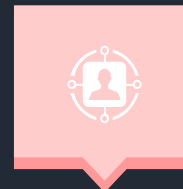
BDAR atitikties kontrolė organizacijos viduje



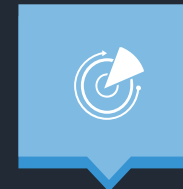
Aukštos duomenų apsaugos kultūros auginimas ir įtvirtinimas



Nešališkas konsultavimas ir geriausių praktikų rekomendavimas



Pagrindinis asmuo kontaktams VDAI



Pagrindinis asmuo kontaktams duomenų subjektams



PRIVACY
PARTNERS

NAUDA ĮMONEI

Kaip panaudoti įmonės BDAR atitiktį
didesniam konkurencingumui ir pelningumui



Privatumas = Organizacijos kultūra



NAUDA

Neužtikrinus **privatumo** prarasite konkurencingumą

Geresnis rinkodaros ROI



Cloud diegimai sistemose



Klientų pasitikėjimas



IT saugos pagerinimas



Skaidrumas verslo procesuose



Atitiktis valstybės
reikalavimams



PRIVACY PARTNERS

Jūsų duomenų apsaugos ekspertai

DAP PASLAUGOS

Duomenų apsaugos
pareigūno priežiūra –
fiksuoja bei pagal poreikį

BDAR AUDITAI

Bendrojo Duomenų Apsaugos
Reglamento situacijos įvertinimas,
rekomendacijos ir atitikties priežiūra

CLOUD ARCHITEKTŪRA

Padėsime įvertinti sistemų perkėlimo į debesį
galimybes ir paruošti kvalifikuotą projektą

PROJEKTŲ VALDYMAS

Padedame parinkti tinkamiausius projekto vykdytojus ir
sistemų diegėjus, prižiūrime projekto eigą ir atstovaujame
klientą IT ir organizaciniais klausimais

IT SAUGA

Įvertiname IT saugos situaciją įmonės sistemose,
tinklapiuose bei infrastruktūroje

[HTTPS://WWW.PRIVACYPARTNERS.LT](https://www.privacypartners.lt)
PAGALBA: BDAR112.LT

• Tel. +370 5 254 8240
• [GDPR112.COM](https://gdpr112.com)

If You think compliance is expensive, try non-compliance

Former US Attorney General Paul McNulty



AČIŪ UŽ DĖMESĮ