



POLITIK FOR BEHANDLING AF PERSONOPLYSNINGER

AFSNIT 1

GENERELLE BESTEMMELSER

1. Walk15, UAB (i det følgende benævnt Virksomhed) Persondatapolitik (i det følgende benævnt Politik) er en del af en offentligt tilgængelig Databehandlingspolitik, der regulerer formålet med behandling af personoplysninger om fysiske personer, hvis data behandles af Virksomheden, fastsætter procedurer for håndhævelse af deres rettigheder, fastsætter de organisatoriske og tekniske databeskyttelsesforanstaltninger og regulerer påberåbelsen af persondataprocessorer.
2. Denne politik er udarbejdet på grundlag af følgende:
 - Lov om retlig beskyttelse af personoplysninger i Republikken Litauen (herefter henvist til LLPPD).
 - Den generelle databeskyttelsesforordning (i det følgende benævnt GDPR).
 - Bekendtgørelse fra Republikken Litauens regering af 28. februar 2001 nr. 228 "Angående godkendelse af vederlagsordren for levering af data til den registrerede og vederlag for dataindsamling fra registrerede dataansvarlige".
 - Anden lovgivning vedrørende behandling og beskyttelse af personoplysninger.
3. Denne politik gælder for automatisk behandling af personoplysninger om fysiske personer samt for manuel behandling af systematiske sæt af personoplysninger. Denne politik fastlægger også rettigheder, forpligtelser og ansvar for virksomhedens medarbejdere i forhold til behandlingen af personoplysninger.
4. Kravene i denne politik er bindende for alle medarbejdere i virksomheden (i det følgende benævnt medarbejdere) og skal også overholdes af databehandlere der, når de leverer databehandlingstjenester til virksomheden, bliver opmærksomme på og behandler personoplysninger, mens de ikke er reguleret af separate aftaler mellem virksomheden og databehandlere.



AFSNIT 2

GENERELLE BEGREBER

5. Personlige data / Data – betyder enhver information, der vedrører en identificeret eller identificerbar fysisk person – direkte eller indirekte, især ved henvisning til en identifikator såsom et navn, en personlig kode, lokaliseringsdata, en online identifikator eller til en eller flere specifikke faktorer til den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sociale identitet hos den fysiske person.
6. Databehandling – betyder enhver operation eller række af operationer, der udføres i en automatiseret eller ikke-automatiseret foranstaltning på personlige data eller personlige datasæt, såsom indsamling, registrering, sortering, systematisering, lagring, tilpasning eller ændring, udtræk, bekendtgørelse, brug, videregivelse ved at transmittere, distribuere eller på anden måde gøre det tilgængeligt for brug, såvel som sammenstilling eller sammenkobling med andre data, begrænsning, sletning eller destruktion.
7. Dataansvarlig – Walk15, UAB, som bestemmer måder og midler til brug af dataene ved behandling af de registreredes data.
8. Registreret – Medarbejdere og andre fysiske personer, hvis data behandles af Walk15, UAB.
9. Databehandler – enheder, der behandler personoplysninger kontrolleret af Walk15, UAB, efter anvisning fra Walk15, UAB i overensstemmelse med indgåede servicekontrakter.
10. Udlevering af data betyder videregivelse af personoplysninger ved overførsel eller på anden måde for at gøre dem tilgængelige (undtagen offentliggørelse i medierne).
11. Mobil applikation – Walk15 mobil applikation administreret af virksomheden.
12. Intern administration – aktiviteter, der sikrer den registeransvarliges selvstændige funktion (strukturforvaltning, personaleforvaltning, forvaltning og anvendelse af tilgængelige materielle og finansielle ressourcer, registrering).
13. Andre udtryk, der anvendes i politikken, skal forstås som defineret i LLPPD og/eller GDPR.

AFSNIT 3

PRINCIPPER OG MÅL FOR BEHANDLING AF PERSONOPLYSNINGER

14. Under udførelsen af deres opgaver og behandlingen af personoplysninger skal personalet:
 - Behandle personoplysninger på en lovlig, retfærdig og gennemsigtig måde.
 - Indsamle data til specificerede, eksplicitte og legitime formål og ikke viderebehandlet på en måde, der er uforenelig med disse formål.



- Overholde principperne om hensigtsmæssighed, proportionalitet og datamængdeminimering ved indsamling og behandling af personoplysninger, ikke kræve levering af data, der ikke er nødvendige, ikke opbevares, og undlad at behandle overskydende data.
 - Sikre nøjagtigheden af personoplysninger og, hvor det er nødvendigt for behandlingen af personoplysninger, holde dem ajour; at korrigere, supplere, slette eller suspendere behandlingen af unøjagtige eller ufuldstændige oplysninger.
 - Opbevare personoplysninger i en form, der tillader identifikation af registrerede ikke længere end nødvendigt for de formål, hvortil oplysningerne blev indsamlet og behandlet.
 - Behandle personoplysninger på en sådan måde, at der sikres tilstrækkelig sikkerhed for personoplysninger ved anvendelse af passende tekniske eller organisatoriske midler, herunder beskyttelse mod uautoriseret behandling eller ulovlig behandling og mod utilsigtet tab, ødelæggelse eller beskadigelse af data (integritets- og fortrolighedsprincippet).
15. Direktøren for regionaludvikling Justina Verbickaitė er ansvarlig for at opdatere oplysningerne om de registrerede i virksomheden.
16. Oplysninger om den registrerede skal gives, hvis loven kræver det.

AFSNIT 5

BEHANDLING AF DATA OM BESKÆFTIGELSESKANDIDATER

- Virksomheden behandler følgende oplysninger om personer, der ønsker at deltage i virksomhedens rekrutteringsproces: navn, efternavn, fødselsdato, adresse, telefon, e-mail, uddannelse, andre oplysninger som angivet i de dokumenter, som ansøgerne har leveret til virksomheden, herunder CV. I tilfælde af at Republikken Litauens lovgivning indeholder yderligere restriktioner for den type oplysninger om ansøgere, der kan behandles, sikrer datakontrolmyndigheden, at kun personoplysninger om ansøgere, der kan behandles, behandles. Følsomme data behandles ikke, medmindre ansøgeren beslutter at levere disse data om sig selv.
17. Grundlaget for databehandlingen er samtykke. Kandidater til de ledige stillinger giver deres samtykke (ved endelig handling) til kun at behandle deres data indtil slutningen af udvælgelsesprocessen. Oplysningerne om ansøgere, der ikke er blevet udvalgt til stillingen (den ledige stilling), slettes ved afslutningen af udvælgelsesproceduren, medmindre de giver deres udtrykkelige samtykke til behandlingen af oplysningerne ved afslutningen af udvælgelsesproceduren.
18. Formålet med databehandling er intern administration. Hvis ansøgerens samtykke til behandlingen af hans data efter afslutningen af udvælgelsesproceduren opnås med det formål at tilbyde et fremtidigt job, behandles oplysningerne på grundlag af samtykke.
19. Kandidater afgiver deres personlige data, når de ansøger til virksomheden. I nogle tilfælde, når stikprøvetagning udføres gennem tredjeparter (Virksomhedens databehandlere), videregives dataene først til dem og først derefter til Virksomheden. I alle tilfælde er virksomheden den dataansvarlige.



20. Kandidatdata må ikke videregives til andre tredjeparter, medmindre kandidaterne anmoder herom, og hvis der er legitime grunde til en sådan videregivelse.

21. Kandidatdata behandles systematisk i virksomhedens databaser, hvortil der er adgang for virksomhedens IT-serviceudbydere. Kandidaternes CV'er eller begrundelsesbreve kan også opbevares i papirform.

22. Kandidater gøres opmærksomme på deres databehandling og deres rettigheder, herunder retten til at ansøge virksomheden om datasletning. Information skal indgå i den politik, der er offentligt tilgængelig på virksomhedens websteder.

AFSNIT 6

OPLYSNINGER OM FYSISKE PERSONER, DER BEHANDLES MED HENBLIK PÅ LEVERING AF TJENESTEYDELSER

23. Virksomheden kan behandle følgende oplysninger om personer, der bruger virksomhedens tjeneste i en mobilapp: navn, efternavn, køn, højde, vægt, skridtlængde, sprog, e-mail, adresse, placering, data, der modtages fra betalingstjenesteudbydere (dvs. Google Pay), samt andre data, der leveres direkte af den registrerede.

24. Tjenestebrugere accepterer vilkårene og betingelserne for brug af virksomhedens administrerede mobilapplikation, før de bruger den. Grundlaget for databehandlingen er indgåelse og opfyldelse af kontrakten.

25. Formålet med databehandling er at levere tjenesterne korrekt.

26. De registrerede indsender selv deres personoplysninger eller giver mobilappen mulighed for at synkronisere data fra Samsung Health, Apple Health Kit eller andre mobilapplikationer. I særlige tilfælde kan data indhentes fra tredjeparter, f.eks. når registrerede foretager køb, dataene kommer fra betalingstjenestevirksomheder eller, når du logger ind med din Google- eller Facebook-konto, kommer dataene direkte fra disse virksomheder.

27. Dataene opbevares i Virksomhedens databaser, som de virksomheder, der leverer IT-tjenester til Virksomheden, har adgang til. Data må ikke videregives til andre tredjeparter, medmindre der fremsættes anmodning herom, og hvis der er legitime grunde til en sådan videregivelse.

Når registrerede bruger visse funktioner i mobilapplikationen (dvs. deltagelse i en udfordring), kan deres data gøres offentligt tilgængelige i mobilapplikationen, men i alle tilfælde kan de deaktivere denne funktion og deltage anonymt.

Data kan også udleveres til tredjeparter, der i samarbejde med Virksomheden offentliggør deres tilbud i Mobilapplikationen ("Step Wallet"). Data leveres, når en mobilapplikationsbruger vælger at bruge funktionen Step Wallet.

28. De registrerede gøres opmærksomme på behandlingen af deres oplysninger og deres rettigheder. Anmeldelse skal ske i politikken som er offentligt tilgængelig Virksomhedens hjemmeside og i den mobile applikation, samt brugsregler, der leveres i den mobile applikation.



AFSNIT 7

DATABEHANDLING MED HENBLIK PÅ DIREKTE MARKEDSFØRING

29. Med henblik på direkte markedsføring behandler virksomheden følgende personoplysninger: navn, efternavn, e-mailadresse. Andre kontaktoplysninger kan også behandles.

30. Databehandlingen er baseret på samtykke.

31. De registrerede indsender selv deres personoplysninger til virksomheden.

32. Dataene opbevares i Virksomhedens databaser, som de virksomheder, der leverer IT-tjenester til Virksomheden, har adgang til. Data må ikke videregives til andre tredjeparter, medmindre der indhentes en anmodning herom fra den registrerede, og hvis der er legitime grunde til en sådan overførsel.

33. Virksomheden behandler ikke mindreåriges data eller følsomme personoplysninger til dette formål. Når virksomheden indsamler data til direkte markedsføringsformål, verificerer virksomheden dog ikke de registreredes alder, da dette ville blive behandlet som en overskydende dataindsamling.

34. De registrerede gøres opmærksomme på deres databehandling og deres rettigheder, herunder retten til at ansøge virksomheden om sletning af data. Meddelelse skal ske i politikken, der offentliggøres på virksomhedens hjemmeside og i mobilapplikationen. Registrerede personer har, efter at den mobile app er downloadet og brugt, ret til at acceptere, at nyhedsbreve om direkte markedsføring sendes til den Registrerede via e-mail eller på anden måde, som den Registrerede tilbyder. Den registrerede har ret til at afmelde eller annullere denne mulighed når som helst.

AFSNIT 8

DATABEHANDLING TIL UNDERSØGELSE, ANMODNING ELLER KLAGEADMINISTRATION, EVALUERING OG UNDERSØGELSE

35. Virksomheden kan behandle følgende oplysninger om de kontaktende fysiske personer til det angivne formål: navn, sprog, e-mailadresse. Virksomheden kan også behandle andre data direkte indhentet fra den registrerede og nødvendige for undersøgelsen, administrationen eller evalueringen af anmodningen, forespørgslen eller klagen.

36. Grundlaget for databehandlingen er indgåelse og opfyldelse af kontrakten.

37. De registrerede indsender selv deres personoplysninger.

38. Dataene opbevares i Virksomhedens databaser, som de virksomheder, der leverer IT-tjenester til Virksomheden, har adgang til. Data må ikke videregives til andre tredjeparter, medmindre der indhentes en anmodning herom fra de registrerede, og hvor der er legitime grunde til en sådan overførsel.

39. De registrerede gøres opmærksomme på behandlingen af deres oplysninger og deres rettigheder. Meddelelse skal gives i politikken, der offentliggøres på virksomhedens hjemmeside og i mobilapplikationen.

AFSNIT 9

COOKIES

40. Virksomheden bruger cookies til at forbedre navigation og tjenester, der leveres af Walk15.com hjemmeside. Virksomhedens hjemmeside kan bruge tredjeparts analytiske cookies- "Google Analytics".

41. Følgende cookies er eller kan blive brugt på virksomhedens hjemmeside.

Navn på cookie	Beskrivelse	Oprettelse søjeblik	Udlø bsdat	Anvendte data
_ga	Et unikt ID logges og bruges til at generere statistik om, hvordan en besøgende bruger	Ved at klikke på knappen "Jeg	2 år	Unik identifikator
_gid	Denne cookie bruges til at skelne brugere.	Ved at klikke på knappen	24 timer	Unik identifikator
_gat*	Disse cookies bruges til at begrænse antallet af anmodninger.	Når du går ind på siden	10 min	Unik identifikator
cookieconsent_status	Bruges til at gemme brugerens samtykke til brugen af cookies.	Ved at klikke på knappen	1 år	Unik identifikator
pll_language	Denne cookie bruges til at gemme den	Når du går ind på siden	1 år	Sprog

42. Virksomheden kan indsamle data om besøgendes handlinger og deres browsing-vaner på en hjemmeside.

43. Du kan få flere oplysninger på: <http://www.google.com/analytics>.

44. Hvis du vil vide, hvordan du deaktiverer sporing på websiderne med Google Analytics-cookies, kan du besøge: <http://tools.google.com/dlpage/gaoptout>.

45. Data videregives til IT-serviceudbydere og Google. Data må ikke videregives til andre tredjeparter, medmindre der fremsættes anmodning herom, og hvis der er legitime grunde til en sådan videregivelse.

46. Hjemmesiden giver dig mulighed for at fravælge brugen af cookies.

AFSNIT 10

VILKÅR FOR DATALAGRING

47. Den dataansvarlige skal anvende følgende frister for opbevaring af personoplysninger:

Nummer	Formålet med behandlingen af personoplysninger	Opbevaringstid
1.	Behandling af medarbejderdata med henblik på intern administration.	Op til 50 år efter ansættelseskontraktens udløb i overensstemmelse med indekset for tilbageholdelsesperioder i Dokumentationsgrundlaget.
2.	Behandling af personoplysninger om jobansøgere.	Indtil afslutningen af udvælgelsen.
3.	Behandling af personoplysninger om jobansøgere efter afslutningen af udvælgelsen finder sted efter indhentning af tilladelse	To år efter modtagelsen af curriculum vitae.
4.	Levering af tjenester.	Data behandles i en periode, der ikke må overstige ti år, som fastsat ved lov.
5.	Administration, evaluering og behandling af anmodninger, undersøgelser eller klager.	6 måneder fra datoen for modtagelsen af anmodningen.
6.	Til direkte markedsføringsformål.	3 år efter indhentning af samtykke.
7.	Cookies til at forbedre kvaliteten af din brug af	Hvor længe en cookie forbliver på din computer afhænger af typen af cookie.

48. Undtagelser fra ovennævnte opbevaringsperioder kan bestemmes i det omfang sådanne undtagelser ikke krænker de registreredes rettigheder, opfylder juridiske krav og er behørigt dokumenteret.

AFSNIT 11

REGISTREREDES RETTIGHEDER OG PROCEDURER FOR DERES GENNEMFØRELSE

Sikring af de registreredes rettigheder og bevidsthed

49. Registrerede personer har ret til:

- At kende (blive informeret) om behandlingen af deres personoplysninger.
- Ved at indsende et identitetsdokument eller ad elektronisk vej, der gør det muligt for personen at blive korrekt identificeret – at få adgang til deres personoplysninger og deres behandling, at indhente oplysninger om kilderne, og hvilke specifikke personoplysninger der indsamles, formålet med behandlingen, modtagerne i det mindste inden for det sidste 1 år, derudover – at modtage en kopi af de dokumenter, der indeholder deres personoplysninger.



- Kræve berigtigelse, sletning eller begrænsning af personoplysninger, bortset fra lagring, hvor behandlingen er i strid med lovkrav.
- At gøre indsigelse mod behandlingen af deres personoplysninger.
- At anmode om overførsel af data til en anden dataansvarlig eller at levere dem direkte til den registrerede i en form, der er praktisk for den registrerede (såsom data, der leveres til virksomheden af den registrerede selv).
- Indgive en klage til tilsynsmyndigheden.
- Tilbagekalde samtykke (hvis personoplysninger behandles på grundlag af samtykke).

50. I alle tilfælde skal virksomheden give den registrerede oplysninger (medmindre den registrerede allerede har sådanne oplysninger) om:

- Navn, retlig enhedskode og hjemsted.
- Eventuelle kontaktoplysninger til den databeskyttelsesansvarlige.
- Til hvilke formål og på hvilket retsgrundlag behandles den registreredes personoplysninger.
- Modtagerne af dataene og deres kategorier.
- Den periode, hvor oplysningerne skal lagres, eller de kriterier, der anvendes til at fastsætte denne periode.
- Andre yderligere oplysninger (om, hvilke personoplysninger den registrerede skal give, og konsekvenserne af undladelse af at give oplysningerne, om den registreredes ret til adgang til sine personoplysninger og hans ret til at rette ukorrekte, ufuldstændige, unøjagtige personoplysninger) i den mængde, der er nødvendig for at sikre korrekt behandling af personoplysninger uden krænkelse af den registreredes rettigheder.
- Kommunikation af hans personoplysninger til tredjemand senest på det tidspunkt, hvor dataene første gang afgives, og hvis den registrerede var uvidende om, at dataene vil blive overført til en anden part.

Bekendtgørelse om gennemførelse af registreredes rettigheder

51. Virksomheden er forpligtet til:

- Gør det muligt for den registrerede at udøve de angivne rettigheder for den registrerede, undtagen i tilfælde, der er fastsat ved lov, når det er nødvendigt for at sikre national sikkerhed eller forsvar, offentlig orden, kriminalitetsforebyggelse, efterforskning, afsløring eller strafferetlig forfølgning, vigtige statslige økonomiske eller finansielle interesser, forebyggelse af overtrædelser af service eller professionel etik, undersøgelse og afsløring heraf, beskyttelse af den registreredes eller andre personers rettigheder og friheder.
- Registrerede skal kontakte virksomhedens filial for at udøve deres rettigheder på følgende kontakter: info@walk15.lt.



- Virksomheden skal sikre, at alle nødvendige oplysninger gives til den registrerede på en klar og forståelig måde.
- Den Registrerede skal svare senest 20 (tyve) arbejdsdage fra datoen for modtagelsen af anmodningen. Hvis den registrerede nægtes adgang til oplysningerne, skal vedkommende have et begrundet svar vedrørende manglende efterlevelse af hans anmodning.

52. Virksomheden skal straks informere de registrerede modtagere af personoplysningerne, som blev korrigeret eller ødelagt på anmodning af den registrerede, om den suspendede behandling af personoplysninger, medmindre det ville være umuligt eller uforholdsmæssigt vanskeligt at levere sådanne oplysninger (på grund af det store antal registrerede, dataperiode, urimeligt høje omkostninger). I så fald skal Statens Datatilsyn straks underrettes.

53. Virksomheden skal levere dataene til den registrerede gratis. I visse tilfælde (når den registrerede klart misbruger sine rettigheder, fremsætter urimeligt gentagne anmodninger om oplysninger, uddrag, dokumenter), kan en sådan udlevering af information og data til den registrerede kræve vederlag i overensstemmelse med lovkrav og de takster, der er fastsat af virksomheden.

Levering af data-til-data-modtagere

54. Virksomheden skal levere den registreredes data i overensstemmelse med kravene i retsakterne og samtidig sikre deres fortrolighed.

55. I tilfælde af levering af engangsdata skal virksomheden prioritere levering af oplysninger ad elektronisk vej.

56. Levering af personoplysninger til statslige og kommunale institutioner og organer, når sådanne institutioner og organer modtager personoplysninger med henblik på udførelsen af de lovpligtige kontrolfunktioner, betragtes ikke som levering af oplysninger til modtagere.

AFSNIT 12

ORGANISATORISKE OG TEKNISKE FORANSTALTNINGER TIL BESKYTTELSE AF PERSONOPLYSNINGER

57. Virksomheden gør sit yderste for at sikre, at virksomhedens organisatoriske og tekniske datasikkerhedsforanstaltninger overholder GDPR-kravene. Følgende infrastruktur-, administrations- og telekommunikationsforanstaltninger (elektroniske) skal træffes for at beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, ændring, videregivelse eller enhver anden ulovlig behandling:

- Korrekt hardwarelayout og -vedligeholdelse, vedligeholdelse af informationssystemer, netværksstyring, sikring af sikkerheden ved brug af internettet og andre informationsteknologiske foranstaltninger:
- Adgang til data og retten til at udføre databehandlingsoperationer gives kun til de Medarbejdere, der har brug for adgang til personoplysningerne i forbindelse med deres opgaver og udførelse af arbejdsopgaver.



- Sikring af sikkerheden i de lokaler, hvor personoplysninger opbevares (kun autoriserede personer har adgang til de pågældende lokaler).
- Efter at have tildelt en computer eller elektronisk kommunikationsenhed til en bestemt medarbejder, skal sådanne computere/elektroniske kommunikationsenheder være beskyttet med adgangskode. Adgangskoder skal ændres med jævne mellemrum, såvel som i tilstedeværelse af visse omstændigheder (ændringer af medarbejder, trussel om hacking, mistanke om, at adgangskoden er blevet kendt af tredjeparter, etc.).
- Sikring af beskyttelse af personoplysninger mod uautoriseret adgang til det interne computernetværk ved hjælp af elektroniske kommunikationsmidler.
- Sikring af anvendelsen af sikre protokoller til overførsel af personoplysninger gennem eksterne datakommunikationsnetværk.
- Streng overholdelse af sikkerhedsstandarder udstedt af sikkerhedstjenesten;
- Korrekt tilrettelæggelse af arbejdet og andre administrative foranstaltninger;
- De nødvendige datasikkerhedsforanstaltninger er installeret under hensyntagen til resultaterne af risikovurderingen;
- Sikkerhedskopiering og gendannelse af data;
- Sikring af, at data gendannes fra de seneste tilgængelige sikkerhedskopier i tilfælde af tab af data på grund af hardwarefejl, softwarefejl eller anden krænkelse af dataintegriteten;
- andre midler.

58. Virksomhedens regionale udviklingschef Justina Verbickaitė er ansvarlig for gennemførelsen, kontrollen og håndhævelsen af disse organisatoriske og tekniske datasikkerhedsforanstaltninger.

59. Medarbejdere, der behandler personoplysninger, skal overholde princippet om fortrolighed og holde alle relevante oplysninger, de har adgang til i forbindelse med deres opgaver, fortrolige. Denne forpligtelse gælder fortsat efter overgang til en anden stilling i virksomheden eller ved ophør af ansættelsesforholdet eller kontraktforholdet med virksomheden.

60. Medarbejdere må kun behandle personoplysninger automatisk, når de har fået adgang til det relevante informationssystem. Adgang til personoplysninger må kun gives til personer, der har brug for personoplysninger for at kunne udføre deres opgaver. Ved ophør af ansættelsesforhold tilbagekaldes Medarbejderens ret til adgang til registre og andre programmer.

61. Medarbejdere må kun overføre dokumenter, der indeholder personoplysninger, til Medarbejdere, der har ret til at arbejde med personoplysninger i henhold til pligter eller særskilte opgaver.



62. Medarbejdere, der udfører den registreredes databehandlingsfunktioner, skal forhindre utilsigtet eller uautoriseret behandling og skal opbevare registre på en korrekt og sikker måde (undgå unødvendig opbevaring af den registreredes data osv.). Kopier af dokumenter, der indeholder oplysninger om den registrerede, skal destrueres på en sådan måde, at indholdet af sådanne dokumenter ikke kan reproducere og deres indhold identificeres.

63. Medarbejdere, hvis computere opbevarer dataene, eller hvis computere er i stand til at kontrollere virksomhedens informationssystemer, hvor dataene er gemt, skal bruge adgangskoder på deres computere; brugerkonti af typen "gæst" i sådanne systemer, dvs. konti uden adgangskode er forbudt. Disse computere skal også bruge en pauseskærm med en adgangskode.

64. Medmindre det er nødvendigt, behøver filer med data ikke kopieres digitalt, dvs. kopier af dem laves til lokale computerdiske, flytbare medier, ekstern fillagring osv.

65. Sikkerhedskontrollen og slettelsen af personoplysninger i eksterne datalagringsmedier og elektronisk post efter deres anvendelse sikres ved at overføre dem til databaser.

66. Regional udviklingschef Justina Verbickaitė skal sikre:

- kontrol af uautoriseret adgang til serverlokaler;
- beskyttelse af Virksomhedens interne computernetværk.

67. Medarbejderne skal tilrettelægge deres arbejde på en sådan måde, at andre personers adgang til de behandlede personoplysninger begrænses mest muligt. Denne bestemmelse skal implementeres:

- Ved at afstå fra at efterlade dokumenter med behandlede personoplysninger eller en computer, der kan åbne filer, der indeholder personoplysninger, uden tilsyn, så oplysninger indeholdt deri kan læses af medarbejdere, der ikke er autoriseret til at arbejde med specifikke personoplysninger, studerende eller andre personer;
- Ved at opbevare dokumenter på en sådan måde, at de (eller deres fragmenter) ikke kan læses af personer ved et uheld;
- Hvis dokumenter, der indeholder personoplysninger, overføres til andre medarbejdere, enheder, filialer, kontorer via personer, der ikke er bemyndiget til at behandle personoplysninger, eller med post eller bud, skal de overføres i en forseglet uigennemsigtig kuvert. Dette stykke finder ikke anvendelse, når sådanne meddelelser udsendes personligt og fortroligt.

68. Regional udviklingschef Justina Verbickaitė er ansvarlig for at håndtere og reagere på brud på persondatasikkerheden.

AFSNIT 13

AFSLUTTENDE BESTEMMELSER

69. Virksomheden har til enhver tid ret til at ændre fortrolighedspolitikken. Ændringerne er gyldige fra det tidspunkt, hvor fortrolighedspolitikken opdateres på webstedet <https://walk15.lt/en/pri-vacy-policy/>. De Registrerede Personer anbefales altid at læse den opdaterede Fortrolighedspolitik.