PATVIRTINTA
AB Akola group
2023-12-19
Valdybos sprendimu Nr. 22

APPROVED
AB Akola Group
19/12/2023
By the Decision of the Board No 22

AB AKOLA GROUP

GRUPĖS ASMENS DUOMENŲ TVARKYMO TAISYKLĖS

AB AKOLA GROUP

GROUP PERSONAL DATA PROCESSING RULES

TURINYS / CONTENTS

1. PAGRINDINĖS SĄVOKOS

1.1. Šiose Asmens duomenų tvarkymo taisyklėse (toliau – **Taisyklės**) didžiąja raide rašomos sąvokos turi žemiau nurodytas reikšmes, išskyrus atvejus, kai kitokią prasmę joms suteikia kontekstas:

Asmens duomenys reiškia bet kokią informaciją apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (Duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.

Asmens duomenų saugumo pažeidimas arba **ADSP** reiškia bet kokį saugumo pažeidimą, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiunčiami, saugomi arba kitaip tvarkomi Asmens duomenys arba prie jų be leidimo gaunama prieiga.

Asmens duomenų tvarkymas reiškia bet kokią automatizuotomis arba neautomatizuotomis priemonėmis su Asmens duomenimis ar Asmens duomenų rinkiniais atliekamą operaciją ar operacijų seką, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

Bendrasis duomenų apsaugos reglamentas arba **BDAR** reiškia 2016 m. balandžio 27 d. Europos parlamento ir tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.

Darbuotojas reiškia asmenį, kuris su bet kuria Grupės įmone yra sudaręs darbo sutartį arba praktikos sutartį (praktikantą), ir apima Grupės įmonių vadovus. Šių Taisyklių tikslais sąvoka „Darbuotojas“ taip pat apima asmenis, kurių su Grupe ar Grupės įmone nesieja darbo santykiai, tačiau kurie dalyvauja Grupės ar Grupės įmonės veikloje ar valdyme (pavyzdžiui, Grupės įmonės priežiūros ir valdymo organų bei komitetų narius, kurie nėra Grupės įmonių darbuotojai).

Duomenų apsaugos pareigūnas arba **DAP** reiškia pagal Bendrojo duomenų apsaugos reglamento 4 skirsnį paskirtą Grupės arba atskirų Grupės įmonių (vienos atskirai ar kelių kartu, priklausomai nuo atvejo) duomenų apsaugos pareigūną, o jei jis nepaskirtas – kitą Grupės ar Grupės įmonės nustatyta tvarka paskirtą asmenį ar įmonę, atsakingą už Asmens duomenų apsaugą Grupėje ar atskirose Grupės įmonėse.

1. MAIN DEFINITIONS

1.1. Capitalised terms used in these Personal Data Processing Rules (the **Rules**) shall have the meanings as set forth hereinbelow unless the context otherwise requires:

Personal Data means any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach or **PDB** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Personal Data Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, as well as alignment or combination, restriction, erasure or destruction.

General Data Protection Regulation or **GDPR** means Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Employee means a person who has an employment contract or an internship contract (apprentice) with any Group Company, including the CEOs of Group Companies. For the purpose of these Rules, the term 'Employee' shall include persons who have no employment relationship with Group or Group Company but who are involved in the business or management of Group or Group Company, for example, in the capacity as members of the Supervisory or Executive Board or committees of Group Company but not as employees of Group Companies.

Data Protection Officer or **DPO** means a data protection officer of Group or of individual Group Companies (alone or in combination with other companies, as the case may be) to be designated in accordance with Section 4 of General Data Protection Regulation, or, if not designated, any other person or entity appointed by Group or Group Company in accordance with the established procedure, to be responsible for the protection of Personal Data within Group or individual Group Companies.

Duomenų subjektas reiškia fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti, ir kurio Asmens duomenis tvarko bet kuri Grupės įmonė.	**Data Subject** means an identified or identifiable natural person whose data shall be processed by any Group Company.
Duomenų tvarkymo veiklos įrašai reiškia kiekvienos Grupės įmonės atžvilgiu DAP pildomą formą, kurioje pateikiama visa informacija apie tos Grupės įmonės tvarkomus Asmens duomenis, tvarkymo tikslus, teisinį pagrindą ir kita teisės aktų reikalaujama pateikti informacija. Jei Duomenų tvarkymo veiklos įrašuose nurodyta informacija skiriasi nuo tos, kuri nurodyta šiose Taisyklėse ar kituose vidiniuose Grupės ar Grupės įmonės dokumentuose, vadovaujamasi Duomenų tvarkymo veiklos įrašuose nurodyta informacija.	**Records of Processing Activities** means a form to be completed by DPO for each Group Company to contain all information about Personal Data processed by Group Company, purposes of processing, legal basis and any other information required by legislation. In the event of any discrepancies between the information contained in Records of Processing Activities and these Rules or other internal documentation of Group or Group Company, the information provided in Records of Processing Activities shall prevail.
Duomenų tvarkytojas reiškia fizinį arba juridinį asmenį, valdžios instituciją, agentūrą ar kitą įstaigą, kuri Grupės ar Grupės įmonės vardu tvarko Asmens duomenis.	**Processor** means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of Group or Group Company.
Duomenų valdytojas reiškia fizinį arba juridinį asmenį, valdžios instituciją, agentūrą ar kitą įstaigą, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones.	**Controller** means a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of processing.
Grupė reiškia įmonių grupę, kurią sudaro Valdymo įmonė ir visos jos tiesiogiai ar netiesiogiai patronuojamos įmonės (nepriklausomai nuo teisinės formos), kuriose Valdymo įmonė tiesiogiai arba netiesiogiai valdo daugiau kaip 25 (dvidešimt penkis) procentus akcijų (dalių, pajų), balsavimo teisių ar teisių į paskirstytinojo pelno dalį arba išimtinių teisių jas įsigyti. Asmens duomenų apsaugos prasme Grupė yra įmonių grupė, kaip ji yra apibrėžta Bendrojo duomenų apsaugos reglamento 4 straipsnio 19 dalyje.	**Group** means a group of companies which consists of Management Company and of its direct or indirect subsidiaries of whatever legal form wherein Management Company holds, directly or indirectly, 25 (twenty-five per cent) of shares (participatory interest, membership interest), voting rights or rights to distributable profits or the exclusive rights to acquire the same. Within the meaning of the protection of Personal Data, Group means a group of companies as defined in Article 4(19) of General Data Protection Regulation.
Grupės įmonė reiškia bet kurią Grupei priklausančią įmonę (nepriklausomai nuo teisinės formos), įskaitant ir Valdymo įmonę.	**Group Company** means any company (of whatever legal form) within Group, including Management Company.
IT saugos specialistas reiškia Grupės ar Grupės įmonės nustatyta tvarka paskirtą asmenį ar asmenis, atsakingus už Grupės informacinių technologijų ir informacijos saugą.	**IT-Security Officer** means a person or persons responsible for Group information technologies and information security appointed by Group or Group Company in accordance with the established procedure .
Kandidatas reiškia fizinį asmenį, pageidaujantį atlikti praktiką ir (ar) įsidarbinti Grupės įmonėje ir sudaryti darbo sutartį.	**Candidate** means a natural person who wishes to take up the internship and/or start working at Group Company under an employment contract.
Priežiūros institucija reiškia: (a) Lietuvos Respublikoje buveines turinčių Grupės įmonių atveju – Lietuvos Respublikos Valstybinę duomenų apsaugos inspekciją, L. Sapiegos g. 17, Vilnius, Lietuvos Respublika (https://vdai.lrv.lt/); (b) Latvijos Respublikoje buveines turinčių Grupės įmonių atveju – Datu Valsts inspekcija, Blaumana g. 11/13-11, Ryga, LV-1011, Latvija (https://www.dvi.gov.lv/), (c) Estijos Respublikoje buveines turinčių Grupės įmonių atveju – Andmekaitse inspektsioon, Tatari g. 39, Talinas 10134, Estija (https://www.aki.ee/).	**Supervisory Authority** means (a) the State Data Protection Inspectorate of the Republic of Lithuania, L. Sapiegos g. 17, Vilnius, the Republic of Lithuania (https://vdai.lrv.lt/) in respect of Group Companies domiciled in the Republic of Lithuania; (b) Datu Valsts inspekcija, Blaumana g. 11/13-11, Riga, LV-1011, Latvia (https://www.dvi.gov.lv/) in respect of Group Companies domiciled in the Republic of Latvia; (c) Andmekaitse inspektsioon, Tatari g. 39, Talinn 10134, Estija (https://www.aki.ee/) in respect of Group Companies domiciled in the Republic of Estonia.
Privatumo politika reiškia privatumo politiką, privatumo pranešimą ar kitą informaciją, kurią Grupė ar Grupės įmonė gali pateikti viešai jų valdomose interneto svetainėse ar socialinės žiniasklaidos paskyrose.	**Privacy Policy** means a privacy policy, privacy notice or any other information placed by Group or Group Company on their websites and social media accounts.
Saugos politika reiškia vieną ar kelis dokumentus, taikomus Grupei ir/ar atskiroms Grupės įmonėms, kuris(-ie) be kita ko	**Security Policy** means one or several documents applicable to the Group and/or separate Group

nustato technines informacijos, įskaitant Asmens duomenis, saugumo priemones.

Specialių kategorijų asmens duomenys reiškia Asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat genetinius, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.

Taikytini teisės aktai reiškia Bendrąjį duomenų apsaugos reglamentą ir nacionalinius asmens duomenų teisinę apsaugą reglamentuojančius bei kitus su Asmens duomenų tvarkymu susijusius įstatymus bei teisės aktus, taikomus Europos Sąjungos valstybėse narėse, kuriose savo buveines turi Grupės įmonės.

Tretysis asmuo reiškia juridinį ar fizinį asmenį, valdžios instituciją, agentūrą ar kitą įstaigą, išskyrus Grupę, Grupės įmones, Darbuotojus, Duomenų subjektą, Duomenų tvarkytoją, arba asmenis, kuriems tiesioginiu Grupės ar Grupės įmonės ar Duomenų tvarkytojo įgaliojimu leidžiama tvarkyti Asmens duomenis.

Trečioji valstybė reiškia ne Europos Sąjungos valstybę narę ir ne Europos Ekonominės Erdvės (EEE) valstybę.

Valdymo įmonė reiškia AB Akola group, juridinio asmens kodas 148030011, buveinė adresu Subačiaus g. 5, 01302 Vilnius, Lietuvos Respublika, kuri šių Taisyklių prasme taip pat yra ir Grupės įmonė.

1.2. Jeigu nenurodyta kitaip, šiose Taisyklėse apibrėžtos sąvokos turi tas pačias reikšmes ir kituose vidiniuose Grupės ir Grupės įmonių dokumentuose, reglamentuojančiuose Asmens duomenų apsaugą.

1.3. Kitos šiose Taisyklėse ir kituose vidiniuose Grupės ir Grupės įmonių dokumentuose, reglamentuojančiuose Asmens duomenų apsaugą, vartojamos sąvokos atitinka Bendrajame duomenų apsaugos reglamente vartojamas sąvokas.

1.4. Nuorodos į punktus, priedus bei kitas nuostatas yra nuorodos į Taisyklių punktus, priedus bei nuostatas.

1.5. Punktų ir kitų nuostatų pavadinimai rašomi tik patogumo sumetimais ir neturi įtakos Taisyklių interpretavimui.

2. BENDROSIOS NUOSTATOS

2.1. Taisyklės reglamentuoja esminius Asmens duomenų tvarkymo Grupėje ir Grupės įmonėse klausimus, Grupės įmonių teises ir pareigas tvarkant Asmens duomenis, nustato kitus su Asmens duomenų tvarkymu susijusius klausimus, užtikrina Taikytinų teisės aktų laikymąsi ir tinkamą įgyvendinimą Grupėje.

2.2. Taisyklės taikomos visoms Grupės įmonėms tiesiogiai ir Grupės įmonės tuo tikslu neturi priimti jokių atskirų lokalinių teisės aktų. Taisyklės yra privalomos visiems Darbuotojams, Grupės įmonių paskirtiems

Companies that determine inter alia information (including Personal Data) technical security measures.

Special Categories of Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Applicable Laws means General Data Protection Regulation, national legislation, and regulations governing the protection of personal data, and any other legislation and regulations on Personal Data Processing as applied in the EU member states where Group Companies are domiciled.

Third Party means a legal or natural person, public authority, agency or body other than Group, Group Companies, Employees, Data Subject, Processor, or persons who, under the direct authority of Group, Group Company or Processor, are authorised to process Personal Data.

Third Country means a non-member state of the European Union and a state outside the European Economic Area (EEA).

Management Company means AB Akola Group, legal entity number 148030011, with its office address at Subačiaus g. 5, LT-01302 Vilnius, the Republic of Lithuania, which is also Group Company within the meaning of these Rules.

1.2. Unless indicated otherwise, terms used in these Rules shall have the same meanings as in internal documents of Group and Group Companies governing Personal Data protection.

1.3. Other terms used in these Rules and in other internal documents of Group and Group Companies governing Personal Data protection shall have the meanings as defined in General Data Protection Regulation.

1.4. Any reference to Sections, Annexes or other provisions shall mean reference to Sections, Annexes, and provisions of these Rules.

1.5. Headings are inserted for convenience only and shall not affect the interpretation of these Rules.

2. GENERAL PROVISIONS

2.1. These Rules shall deal with material issues relating to Personal Data Processing within Group and Group Companies, Group Companies' rights and obligations with regard to Personal Data Processing, regulate other matters associated with Personal Data Processing, and ensure the compliance with and duly implementation of Applicable Laws within Group.

2.2. These Rules shall apply to all Group Companies directly and Group Companies shall not individually adopt any local regulations to that effect. Rules shall be binding on all Employees, Processors appointed by

Duomenų tvarkytojams ir jų darbuotojams ar kitiems atstovams, tvarkantiems Asmens duomenis, nepriklausomai nuo jų priėmimo į darbą sąlygų. Taisyklės taip pat taikomos visiems Grupės ar Grupės įmonių paskirtiems ekspertams (konsultantams) ir kitiems asmenims, kurie, eidami savo pareigas, sužino bet kurios Grupės įmonės tvarkomus Asmens duomenis.

2.3. Kiekviena Grupės įmonė supažindina su Taisyklėmis savo Darbuotojus Taisyklių 11 dalyje nustatyta tvarka.

3. ASMENS DUOMENŲ TVARKYMAS. PAGRINDINIAI VAIDMENYS

3.1. Grupės įmonės gali tvarkyti Asmens duomenis kaip Duomenų valdytojai arba kaip Duomenų tvarkytojai. Grupės įmonės taip pat turi teisę pasitelkti Duomenų tvarkytojus.

3.2. **Duomenų valdytojas**. Kai Grupės įmonė veikia kaip Duomenų valdytojas, ji, vadovaudamasi šiomis Taisyklėmis ir Taikytinais teisės aktais, nustato Asmens duomenų tvarkymo tikslus ir priemones, saugojimo terminus, parenka tokiam tvarkymui tinkamą teisinį pagrindą.

3.3. **Bendri valdytojai**. Tais atvejais, kai dvi ar daugiau Grupės įmonių kartu nustato Asmens duomenų tvarkymo tikslus ir priemones, jos yra bendri Duomenų valdytojai, kaip tai numato Bendrojo duomenų apsaugos reglamento 26 straipsnis. Tokiu atveju Grupės įmonės, kurios yra bendri Duomenų valdytojai, turi sudaryti rašytinį susitarimą, kuriame be kita ko skaidriu būdu turi nustatyti:

3.3.1. tvarką, kaip bus įgyvendinamos Duomenų subjektų teisės; susitarimu gali būti paskirtas Duomenų subjektų informavimo punktas;

3.3.2. tvarką, kaip bus pateikiama Bendrojo duomenų apsaugos reglamento 13 ir 14 straipsniuose nurodyta informacija (santrauka pateikiama Taisyklių 2 priede);

3.3.3. savo atitinkamą atsakomybę už kitų Taikytinuose teisės aktuose nustatytų prievolių vykdymą, jeigu reikia.

3.4. **Duomenų tvarkytojas**. Jeigu Grupės įmonė tvarko Asmens duomenis Duomenų valdytojo nurodymu, ji veikia kaip Duomenų tvarkytojas. Viena Grupės įmonė gali būti kitos Grupės įmonės, kaip Duomenų valdytojo, Duomenų tvarkytoju. Grupės įmonei veikiant kaip Duomenų tvarkytojas, laikomasi šių reikalavimų:

3.4.1. Grupės įmonė, tvarkydama Asmens duomenis kaip Duomenų tvarkytojas, vadovaujasi su Duomenų valdytoju sudaryta Asmens duomenų tvarkymo sutartimi.

3.4.2. kiti Grupės įmonei, kaip Duomenų tvarkytojui, keliami reikalavimai, numatyti Bendrojo duomenų apsaugos reglamento 28 straipsnyje.

3.4.3. Darbuotojai, tvarkydami Duomenų valdytojo perduotus Asmens duomenis, visais atvejais privalo įsitikinti ketinamų atlikti veiksmų teisėtumu, vadovaujantis Grupės

Group Companies, and on Processors' employees or representatives who process Personal Data, irrespective of the terms and conditions of their employment. These Rules shall also apply to all experts (consultants) appointed by Group or Group Companies and to other persons who, in the performance of their duties, have access to Personal Data processed by any Group Company.

2.3. Each Group Company shall make these Rules available to its Employees in accordance with Section 11 hereof.

3. PERSONAL DATA PROCESSING. KEY ROLES

3.1. Group Companies may process Personal Data in their capacity as Controllers or Processors. Group Companies may also involve Processors.

3.2. **Controller.** Where Group Company acts as Controller it shall determine the purposes and means of Personal Data Processing, data storage time, and the legal basis for processing in accordance with these Rules and Applicable Laws.

3.3. **Joint Controllers**. Where two or more Group Companies jointly determine the purposes and means of Personal Data Processing, they shall be Joint Controllers under Article 26 of General Data Protection Regulation. In such a case, Group Companies who are Joint Controllers shall enter into a written agreement whereby they shall, *inter alia*, in a transparent manner determine the following:

3.3.1. the procedure for exercising of the rights of Data Subjects; the agreement may designate a contact point for Data Subjects;

3.3.2. the procedure for provision of the information referred to in Articles 13 and 14 of General Data Protection Regulation (summary provided in Annex 2 to the Rules);

3.3.3. their respective responsibilities for the compliance with other obligations under Applicable Laws, if applicable.

3.4. **Processor**. Group Company may also act as Processor where it processes Personal Data under the instruction of Controller. A Group Company may be Processor of another Group Company in its capacity as Controller. Group Company in its capacity as Processor shall abide by the following:

3.4.1. in processing Personal Data in its capacity as Processor, Group Company shall act in accordance with Personal Data Processing Agreement made with Controller;

3.4.2. other requirements applicable to Group Company in its capacity as Processor are provided for in Article 28 of General Data Protection Regulation.

3.4.3. in processing Personal Data transferred by Controller, Employees shall in all cases verify the lawfulness of intended actions in accordance with the

įmonės ir Duomenų valdytojo sudaryta sutartimi ir joje aptartais Asmens duomenų tvarkymo ribojimais ir tvarka.

3.5. **Duomenų tvarkytojo pasitelkimas**. Prieš pasitelkdama Duomenų tvarkytoją Grupės įmonė turi: (a) įsitikinti, kad Duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines saugumo priemones ir atitinka šių Taisyklių bei Bendrojo duomenų apsaugos reglamento reikalavimus, ir (b) sudaryti Asmens duomenų tvarkymo sutartį. Siekdama įsitikinti Duomenų tvarkytojo atitiktimi šių Taisyklių bei Bendrojo duomenų apsaugos reglamento reikalavimams, Grupės įmonė kiekvieno Duomenų tvarkytojo prašo pateikti dokumentais pagrįstus atitinkamus įrodymus. Esant aukštesniam rizikos lygiui, Duomenų apsaugos pareigūnas gali reguliariai tikrinti Duomenų tvarkytojo atitiktį minėtiems reikalavimams.

3.6. **Asmens duomenų tvarkymo sutartis**. Asmens duomenų tvarkymo sutarties reikalavimai yra įtvirtinti Bendrojo duomenų apsaugos reglamento 28 straipsnio 3 dalyje. Valdymo įmonė parengia ir patvirtina Asmens duomenų tvarkymo sutarties projektą (formą), kurį kiekviena Grupės įmonė siekia naudoti, pasirašant Asmens duomenų tvarkymo sutartis su visais Duomenų tvarkytojais (kai tai yra objektyviai įmanoma). Šį sutarties projektą (formą) Duomenų apsaugos pareigūnas peržiūri ir atnaujina pagal poreikį. Prieš pasirašant kiekvieną Asmens duomenų tvarkymo sutartį, ją turi peržiūrėti ir patvirtinti Duomenų apsaugos pareigūnas.

4. ASMENS DUOMENŲ TVARKYMO PRINCIPAI

4.1. Grupė ir kiekviena Grupės įmonė tvarko Asmens duomenis vadovaudamasi šiais principais:

(a) Duomenų subjekto atžvilgiu Asmens duomenys tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);

(b) Asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau nebetvarkomi su tais tikslais nesuderinamu būdu (tikslo apribojimo principas);

(c) Asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų mažinimo principas);

(d) Asmens duomenys turi būti tikslūs ir prireikus atnaujinami (tikslumo principas);

(e) Asmens duomenys laikomi tokia forma, kad Duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau nei tai yra būtina tais tikslais, kuriais Asmens duomenys yra tvarkomi (saugojimo trukmės apribojimo principas);

(f) Asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas Asmens duomenų saugumas, įskaitant apsaugą nuo Asmens duomenų

provisions of the agreement made by and between Group Company and Controller and with the restrictions and procedures discussed therein.

3.5. **Engagement of Processor**. Prior to engaging Processor, Group Company shall (a) satisfy itself that Processor implements appropriate technical and organisational security measures and complies with the requirements of these Rules and of General Data Protection Regulation, and (b) enter into Personal Data Processing Agreement. In order to determine whether Processor fulfils the requirements laid down in these Rules and in General Data Protection Regulation, Group Company shall ask for documented evidence to be submitted by each Processor. In the event of a higher level of risk, Data Protection Officer shall have the right to check on a regular basis Processor's compliance with the said requirements.

3.6. **Personal Data Processing Agreement**. Requirements for the Personal Data Processing Agreement are established in Article 28(3) of General Data Protection Regulation. A draft (template) of Personal Data Processing Agreement to be used by each Group Company with all Processors shall be drawn up and approved by Management Company, where objectively possible. The draft (template) shall be revised and, where applicable, updated by Data Protection Officer. No Personal Data Processing Agreement shall be signed unless reviewed and approved by Data Protection Officer.

4. PERSONAL DATA PROCESSING PRINCIPLES

4.1. Group and each Group Company shall process Personal Data pursuant to the following principles:

(a) Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to Data Subject (the principle of lawfulness, fairness and transparency);

(b) Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the principle of purpose limitation);

(c) Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (the principle of data minimisation);

(d) Personal Data shall be accurate and, where necessary, kept up to date (the principle of accuracy);

(e) Personal Data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which they are processed (the principle of storage limitation);

(f) Personal Data shall be processed in a manner that ensures appropriate security thereof, including protection against unauthorised or unlawful processing and against accidental loss,

tvarkymo be leidimo arba neteisėto Asmens duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas);

(g) Grupė ir Grupės įmonės įgyvendina Taikytinų ir Taikytinų teisės aktų reikalavimus, darbuotoi jų laikymąsi ir kaupia duomenis Bendrojo duomenų apsaugos reglamento ir kitų Taikytinų teisės aktų reikalavimų atitikčiai įrodyti (atskaitomybės principas).

4.2. Papildomai prie Taisyklių 4.1 punkto, Grupė ir Grupės įmonės, tvarkydamos Darbuotojų Asmens duomenis, vadovaujasi šiais pagrindiniais principais:

(a) Darbuotojas yra silpnesnioji darbo santykio šalis, jo sutikimas negali būti pakankamas teisinis pagrindas tvarkyti daugumą Asmens duomenų rūšių;

(b) Darbuotojo Asmens duomenų tvarkymas gali būti reikalingas darbo sutarčiai vykdyti ir tam, kad Grupės įmonė, kurios Darbuotojas jis yra, galėtų įgyvendinti savo įsipareigojimus;

(c) Grupės įmonei, kaip darbdaviui, gali būti nustatyti teisiniai įpareigojimai, pagal kuriuos Darbuotojo Asmens duomenų tvarkymas yra neišvengiamas;

(d) jei Grupės įmonė deklaruoja teisėtą interesą tvarkyti Darbuotojo Asmens duomenis, Asmens duomenų tvarkymo tikslas turi būti teisėtas; pasirinktas metodas ir (ar) specifinė technologija turi būti būtini, proporcingi ir įgyvendinami su kuo mažesniu poveikiu, taip pat turi būti atliktas teisėto intereso vertinimas, kaip tai numatyta Grupės Teisėto intereso įvertinimo procedūroje;

(e) Asmens duomenų tvarkymo operacijos turi atitikti skaidrumo reikalavimus, o Darbuotojai turi būti aiškiai ir išsamiai informuoti apie jų Asmens duomenų tvarkymą, įskaitant bet kokios stebėsenos egzistavimą;

(f) Grupė ir Grupės įmonės imasi techninių ir organizacinių priemonių saugiam Darbuotojų Asmens duomenų tvarkymui užtikrinti.

5. DUOMENŲ APSAUGOS PAREIGŪNAS (DAP)

5.1. Kadangi, vadovaujantis Bendrojo duomenų apsaugos reglamento 37 straipsnio 2 dalimi, įmonių grupė gali paskirti vieną Domenų apsaugos pareigūną, jeigu su juo lengva susisiekti iš kiekvienos buveinės, Valdymo įmonės sprendimu Grupėje paskiriamas Grupės Duomenų apsaugos pareigūnas. Kiekviena Grupės įmonė ar kelios Grupės įmonės kartu taip pat gali paskirti atskirą tos Grupės įmonės ar kelių Grupės įmonių Duomenų apsaugos pareigūną.

destruction or damage, using appropriate technical or organisational measures (the principle of integrity and confidentiality);

(g) Group and Group Companies shall implement legal requirements set out in these Rules and Applicable Laws, monitor compliance with such requirements, and shall collect data to prove compliance with the requirements of General Data Protection Regulation and other Applicable Laws (the principle of accountability).

4.2. In addition to Section 4.1 hereof, Group and Group Companies shall process Employees' Personal Data pursuant to the following key principles:

(a) Employee is the weaker party in the employment relationship and his/her consent cannot be considered sufficient legal basis for the processing of most types of Personal Data;

(b) the processing of Employee's Personal Data is necessary for the performance of an employment contract and for the fulfilment of obligations of Group Company within which such Employee is employed;

(c) legal obligations imposed on Group Company, in its capacity as the employer, makes the processing of Employee's Personal Data unavoidable;

(d) if Group Company pursues the legitimate interest in the processing of Employee's Personal Data, the purpose of Personal Data Processing must be lawful; the selected method and/or specific technology must be necessary, proportionate and implementable with as low impact as possible, and, in addition, the assessment of the legitimate interest must be carried out as prescribed by Group's Procedure for the Assessment of Legitimate Interest;

(e) Personal Data Processing operations must comply with the transparency requirements, and Employees must be explicitly and comprehensively informed about their Personal Data Processing, including about the existence of any monitoring;

(f) Group and Group Companies will implement technical and organisational measures in order to ensure the safe processing of Employees' Personal Data.

5. DATA PROTECTION OFFICER (DPO)

5.1. Since, pursuant to Article 37(2) of General Data Protection Regulation, a group of companies may appoint a single Data Protection Officer provided that such Data Protection Officer is easily accessible from each establishment, Data Protection Officer shall be appointed within Group by decision of Management Company. Each Group Company or several Group

Companies jointly may also appoint its own or their own Data Protection Officer.

5.2. Jeigu Grupėje yra paskirtas Grupės Duomenų apsaugos pareigūnas, jis prižiūri visos Grupės ir Grupės įmonių atitiktį Taikytiniems teisės aktams bei Duomenų subjektų prašymų įgyvendinimą, konsultuoja asmens duomenų apsaugos klausimais, bendradarbiauja su priežiūros institucija. Jeigu yra paskiriami atskirų Grupės įmonių (vienos ar kelių) Duomenų apsaugos pareigūnai, jie yra atsakingi už atitinkamų Grupės įmonių atitikties Taikytiniems teisės aktams priežiūrą, Duomenų subjektų prašymų įgyvendinimą, konsultavimą asmens duomenų apsaugos klausimais, bendradarbiavimą su priežiūros institucija. Tokiu atveju Grupėje veikiančių Duomenų apsaugos pareigūnų pareigų pasiskirstymą reglamentuoja Valdymo įmonės ir atitinkamų Grupės įmonių, kuriose tokie Duomenų apsaugos pareigūnai yra paskirti, bendrai nustatyta tvarka.

5.2. If Data Protection Officer is appointed within Group, such Data Protection Officer shall be responsible for the compliance by Group and Group Companies with Applicable Laws and requests from Data Subjects. Where Group Companies (one or several) appoint their own Data Protection Officers, they shall be responsible for the compliance by relevant Group Companies with Applicable Laws and requests from Data Subjects. In such a case, the distribution of responsibilities between Data Protection Officers within Group shall be governed by the procedure adopted jointly by Management Company and Group Companies within which Data Protection Officers operate.

5.3. Darbuotojai ir Duomenų subjektai turi teisę tiesiogiai kreiptis į Duomenų apsaugos pareigūną(-us) visais su jų Asmens duomenų tvarkymu susijusiais klausimais.

5.3. Employees and Data Subjects shall have the right to contact Data Protection Officer(s) directly on any matter related to their Personal Data Processing.

6. DUOMENŲ TVARKYMO VEIKLOS ĮRAŠAI

6. RECORDS OF PROCESSING ACTIVITIES

6.1. Kiekviena Grupės įmonė tvarko tokios Grupės įmonės Duomenų tvarkymo veiklos įrašus.

6.1. Each Group Company shall maintain its Records of Processing Activities.

6.2. Duomenų tvarkymo veiklos įrašuose pateikiama aktuali (nuolat atnaujinama) informacija apie konkrečios Grupės įmonės tvarkomus Asmens duomenis, jų tvarkymo tikslus, Asmens duomenų tvarkymo tvarką, apimtis ir terminus, kita informacija, nurodyta Bendrojo duomenų apsaugos reglamento 30 straipsnyje. Už Duomenų tvarkymo veiklos įrašų pildymą yra atsakingas tos Grupės įmonės Duomenų apsaugos pareigūnas, o jeigu Grupės įmonė neturi atskiro Duomenų apsaugos pareigūno, - Grupės Duomenų apsaugos pareigūnas.

6.2. Records of Processing Activities shall contain relevant (up-to-date) information on Personal Data processed by specific Group Company, the purposes, procedure, scope and time limits of Personal Data Processing as well as other information specified in Article 30 of General Data Protection Regulation. Completion of Records of Processing Activities shall be under the responsibility of Data Protection Officer of that specific Group Company or, where Group Company does not have a separate Data Protection Officer, the responsibility shall fall under Group's Data Protection Officer.

6.3. Grupės įmonė, gavusi Priežiūros institucijos prašymą, Duomenų tvarkymo veiklos įrašus pateikia nedelsdama.

6.3. Records of Processing Activities shall be immediately submitted by Group Company at Supervisory Authority's request.

7. ASMENS DUOMENŲ TVARKYMO TIKSLAI IR TVARKOMI ASMENS DUOMENYS

7. PURPOSES OF PROCESSING OF PERSONAL DATA AND PROCESSED PERSONAL DATA

7.1. Baigtinis kiekvienos Grupės įmonės tvarkomų Asmens duomenų sąrašas yra pateikiamas tos Grupės įmonės Duomenų tvarkymo veiklos įrašuose.

7.1. An exhaustive list of Personal Data processed by each Group Company shall be given in Records of Processing Activities.

7.2. Asmens duomenų tvarkymas kitais tikslais nei tais, kuriais iš pradžių buvo rinkti Asmens duomenys, turėtų būti leidžiamas tik tuomet, kai Asmens duomenų tvarkymas suderinamas su tikslais, kuriais iš pradžių buvo rinkti Asmens duomenys.

7.2. Personal Data Processing for purposes other than those for which Personal Data were initially collected should be allowed only where the processing is compatible with the purposes for which Personal Data were initially collected.

7.3. Jei Darbuotojas, savo darbo veikloje ar kito Darbuotojo nurodymu, ketina vykdyti veiklą Grupės ar Grupės įmonės vardu ar interesais dėl kurios:

7.3. Where Employee, in the performance of his/her work duties or on instruction from any other Employee, intends to engage in the activity on behalf or in the interest of Group or Group Company, which activity would:

7.3.1. atsirastų naujas Asmens duomenų tvarkymo tikslas, neįtrauktas į Duomenų tvarkymo veiklos įrašus; arba

7.3.2. atsirastų naujas Asmens duomuo, neįtrauktas į Duomenų tvarkymo veiklos įrašus (nepriklausomai ar tai naujas tikslas); arba

7.3.3. iš esmės pasikeistų operacijos su Asmens duomenimis pobūdis,

Darbuotojas prieš pradėdamas tokią veiklą privalo informuoti Duomenų apsaugos pareigūną ir konsultuotis dėl tokios naujos duomenų tvarkymo operacijos. Darbuotojas negali pradėti vykdyti naujos veiklos negavęs Duomenų apsaugos pareigūno patvirtinimo.

8. ASMENS DUOMENŲ TVARKYMO TEISINIAI PAGRINDAI

8.1. Grupės įmonės tvarko Asmens duomenis esant bent vienam šių pagrindų:

8.1.1. Duomenų subjekto sutikimas;

8.1.2. Grupės įmonės su Duomenų subjektu sudarytų sutarčių vykdymas, arba siekis imtis veiksmų Duomenų subjekto prašymu prieš sudarant sutartį;

8.1.3. Grupės įmonei taikomų teisinių prievolių, įskaitant bet neapsiribojant Grupės įmonių teisines prievoles darbo teisės ir socialinės apsaugos srityje, vykdymas;

8.1.4. siekiant apsaugoti gyvybinius Duomenų subjekto ar kito fizinio asmens interesus;

8.1.5. tvarkyti Asmens duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant Grupės įmonei pavestas viešosios valdžios funkcijas;

8.1.6. tvarkyti Asmens duomenis būtina, siekiant teisėtų Grupės įmonės arba Trečiojo asmens interesų.

8.2. **Sutikimas, kaip Asmens duomenų tvarkymo teisinis pagrindas**

8.2.1. Tais atvejais, kai netaikomas joks kitas toliau šioje Taisyklių dalyje nurodytas ir Bendrajame duomenų apsaugos reglamente nustatytas teisinis pagrindas Asmens duomenų tvarkymui, Asmens duomenys gali būti tvarkomi tik gavus išankstinį Duomenų subjekto sutikimą. Prieš renkantis Duomenų subjekto sutikimą, kaip Asmens duomenų tvarkymo teisinį pagrindą, Grupės įmonė turi įvertinti kitų teisinių pagrindų taikymo galimybes.

8.2.2. Sutikimas turėtų būti duodamas aiškiu aktu patvirtinant, kad yra suteiktas laisva valia, konkretus, informacija pagrįstas ir vienareikšmis nurodymas, kad Duomenų subjektas sutinka, kad būtų tvarkomi su juo susiję Asmens duomenys, pavyzdžiui, raštiškas, įskaitant elektroninėmis priemonėmis. Tylėjimas, neveikimas, iš anksto pažymėti langeliai, langeliai, kuriuos būtina pažymėti siekiant neduoti sutikimo (angl. opt-out boxes), standartiniai nustatymai, bendro pobūdžio sutikimas ir kitos panašios priemonės nėra laikomos sutikimo davimu. Žodinis sutikimas gali būti duodamas tik tuo atveju, jei neabejotinai

7.3.1. create a new purpose of processing not included in Records of Processing Activities; or

7.3.2. create a new element of Personal Data not included in Records of Processing Activities (irrespective of the fact if this is for a new purpose); or

7.3.3. materially change the nature of operation performed on Personal Data,

prior to initiating such activity, Employee shall inform Data Protection Officer and obtain a consultation on such new data processing operation. Any new activity to be taken by Employee shall be subject to the approval by Data Protection Officer.

8. LEGAL BASIS FOR PERSONAL DATA PROCESSING

8.1. Group Companies shall process Personal Data if at least one of the following bases is present:

8.1.1. Data Subject has given his/her consent;

8.1.2. it is necessary for the performance of agreements made by Group Companies with Data Subject or for steps to be taken at Data Subject's request prior to entering into an agreement;

8.1.3. it is necessary for the compliance with legal obligations applicable to Group Company, including, but not limited to, the legal obligations of Group Companies in the areas of employment law and social security;

8.1.4. it is necessary for protection of vital interests of Data Subject or of another natural person;

8.1.5. it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Group Company;

8.1.6. it is necessary for the purpose of legitimate interests of Group Company or of Third Party.

8.2. **Consent as the legal basis for Personal Data Processing**

8.2.1. In the event no other legal basis for Personal Data Processing as indicated further in this Section and provided for in General Data Protection Regulation is applicable, Personal Data may be processed only having obtained a prior consent of the Data Subject. Before choosing Data Subject's consent as legal basis for Personal Data Processing, Group Company shall evaluate the possibility to apply other legal bases.

8.2.2. Consent should be given by a clear affirmative act, such as by a written statement, including by electronic means, establishing a freely given, specific, informed and unambiguous indication of Data Subject's agreement to the processing of his/her Personal Data. Silence, inactivity, pre-ticked boxes, opt-out boxes, default settings, general consent and other similar measures shall not be considered to constitute consent. Verbal consent may be given only in cases where it is possible to undoubtedly prove the fact of provision of such verbal consent. Should there be any doubts as to

įmanoma įrodyti tokio žodinio sutikimo davimo faktą. Jei kyla abejonės dėl gebėjimo įrodyti žodinio sutikimo davimą, visada rekomenduojama gauti rašytinį sutikimą.

8.2.3. Sutikimas yra „informacija pagrįstas“, kai prieš prašant sutikimo Duomenų subjektui yra pateikiama informacija, nurodyta Bendrojo duomenų apsaugos reglamento 13 arba 14 straipsnyje (santrauka pateikiama Taisyklių 2 priede). Grupės įmonė, prieš prašydama sutikimo, turi pateikti Duomenų subjektui tokią informaciją.

8.2.4. Daugeliu atveju, esant kitiems teisėtiems Asmens duomenų tvarkymo pagrindams, Darbuotojų Asmens duomenų tvarkymo teisinis pagrindas negali būti sutikimas. Net ir esant Darbuotojo sutikimui, gali būti pripažinta, kad Grupės įmonė, kaip darbdavys, neturi teisėto pagrindo tvarkyti Darbuotojo Asmens duomenis dėl Grupės įmonės ir Darbuotojo padėties disbalanso.

8.2.5. Toliau pateikiami galimų sutikimo gavimo būdų pavyzdžiai (gali būti naudojami ir kiti būdai, jeigu neabejotinai įmanoma įrodyti tokio sutikimo davimo faktą):

(a) raštiško pareiškimo dėl sutikimo pasirašymas;

(b) pažymint langelį dėl sutikimo popierinėje ar elektroninėje formoje;

(c) paspaudžiant sutikimo nuorodą ar mygtuką interneto naršyklės lange, mobiliojoje programėlėje ar pan. Tokiu atveju patartina naudoti el. pašto patvirtinimo funkciją (angl. double opt-in);

(d) pasirinkus iš vienodai gerai matomų taip/ne pasirinkčių;

(e) atsakius į elektroninį laišką, kuriuo prašoma sutikimo (jei Grupės įmonė turi teisę siųsti tokio pobūdžio laiškus; plačiau apie tiesioginės rinkodaros pranešimus žr. Taisyklių 10.2 punkte).

8.2.6. Jeigu Duomenų subjekto sutikimas duodamas rašytiniu pareiškimu, susijusiu ir su kitais klausimais, prašymas duoti sutikimą pateikiamas tokiu būdu, kad jis būtų aiškiai atskirtas nuo kitų klausimų, pateiktas suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba.

8.2.7. Rašytinio sutikimo tekstas visada turi būti derinamas su DAP ir gali būti naudojamas tik DAP patvirtinus jo formą. Toks patvirtinimas galimas ir elektroniniu paštu.

8.2.8. Sutikimas turėtų apimti visą Asmens duomenų tvarkymo veiklą, vykdomą tuo pačiu tikslu ar tais pačiais tikslais. Kai Asmens duomenys tvarkomi ne vienu tikslu, sutikimas turėtų būti duotas dėl visų duomenų tvarkymo tikslų.

8.2.9. Duomenų subjektas turi teisę bet kuriuo metu atšaukti savo sutikimą. Sutikimo atšaukimas nedaro poveikio sutikimu pagrįsto Asmens duomenų tvarkymo, atlikto iki sutikimo atšaukimo, teisėtumui (t. y. iki sutikimo atšaukimo teisėtai sutikimo pagrindu tvarkyti Asmens duomenys neturi būti ištrinami ar kitaip naikinami). Duomenų subjektas apie tai informuojamas prieš jam

the ability to prove the provision of verbal consent, it is always recommended that a written consent be obtained.

8.2.3. ‘Informed consent’ is when prior to asking for consent Data Subject is provided with the information specified in Article 13 or Article 14 of General Data Protection Regulation (summary provided in Annex 2 to the Rules). Before asking for consent, Group Company shall submit the said information to Data Subject.

8.2.4. In most cases, where there are other lawful bases for Personal Data Processing, the consent cannot be treated as legal basis for Employees’ Personal Data Processing. Even if Employee has given his/her consent, it may be considered that Group Company, as the employer, has no lawful basis for Employee’s Personal Data Processing in case where there is an imbalance between Group Company and Employee.

8.2.5. The following are examples of ways to obtain the consent (other ways may be used provided that it is possible to undoubtedly prove the fact of provision of such consent):

(a) signing a written consent statement;

(b) ticking an opt-in box on paper or electronically;

(c) clicking an opt-in button or link online or using mobile application, etc. In this case it is recommended to use e-mail verification (double opt-in) process;

(d) selecting from equally prominent yes/no options;

(e) responding to an e-mail requesting consent (if Group Company has the right to send such e-mails; for more information on direct marketing communication see Section 10.2 of the Rules).

8.2.6. If Data Subject's consent is given in the form of written statement which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

8.2.7. The text of written consent shall always be agreed with DPO and may be used only upon the approval by DPO. Such approval may also be given by e-mail.

8.2.8. Consent should cover all Personal Data Processing activities carried out for the same purpose or purposes. Where Personal Data Processing has multiple purposes, consent should be given for all of them.

8.2.9. Data Subject shall have the right to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of Personal Data Processing based on consent before its withdrawal (i.e., Personal Data lawfully processed based on consent until its withdrawal shall not be deleted or otherwise destroyed), and Data Subject shall be informed to that

duodant sutikimą. Atšaukti sutikimą turi būti taip pat lengva, kaip jį duoti.

8.3. **Sutarties vykdymas, kaip Asmens duomenų tvarkymo teisinis pagrindas**

8.3.1. Sutarties vykdymas ar pasirengimas ją vykdyti gali būti teisėtu Asmens duomenų tvarkymo pagrindu tik tuomet, kai tvarkomi Asmens duomenys yra būtini pasirengimui su Duomenų subjektu sudaryti sutartį ar ją vykdyti.

8.3.2. Sutarties vykdymas ar pasirengimas ją vykdyti gali būti teisėtu Asmens duomenų tvarkymo pagrindu tik tuomet, kai ir Duomenų subjektas, ir Grupės įmonė yra (bus) tokios sutarties šalys.

8.4. **Teisinė prievolė, kaip Asmens duomenų tvarkymo teisinis pagrindas**

8.4.1. Grupės įmonės tvarko Asmens duomenis, siekdamos įgyvendinti joms nustatytas prievoles, įskaitant, bet neapsiribojant, darbo teisės ir socialinės apsaugos srityje, kurias nustato Taikytini teisės aktai.

8.4.2. Asmens duomenų tvarkymo tikslus, apimtis, terminus, kitas sąlygas nustato Taikytini teisės aktai.

8.4.3. Teisinė prievolė gali būti teisėtu Asmens duomenų tvarkymo pagrindu tik tuomet, kai Asmens duomenų tvarkymas aiškiai, o ne abstrakčiai, įtvirtintas Taikytinuose teisės aktuose.

8.5. **Gyvybiniai interesai, kaip Asmens duomenų tvarkymo teisinis pagrindas**

8.5.1. Asmens duomenų tvarkymas, siekiant apsaugoti gyvybinius interesus, turi būti būtinas. Jei asmuo gali duoti sutikimą, šiuo Asmens duomenų tvarkymo pagrindu remtis negalima.

8.6. **Užduotis viešojo intereso labui arba viešųjų funkcijų vykdymas**

8.6.1. Remtis Asmens duomenų tvarkymo pagrindu, kai tvarkyti Asmens duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant Grupės įmonei, kaip Duomenų valdytojui, pavestas viešosios valdžios funkcijas, galima tik tuomet, kai tai yra nustatyta Taikytinuose teisės aktuose.

8.7. **Teisėtas interesas, kaip Asmens duomenų tvarkymo teisinis pagrindas**

8.7.1. Grupės įmonei tvarkant Asmens duomenis teisėto intereso pagrindu, Asmens duomenų tvarkymo tikslas turi būti teisėtas, o Asmens duomenų tvarkymo metodas ar technologija turi būti reikalinga Grupės įmonės interesams pasiekti. Asmens duomenų tvarkymas taip pat turi būti proporcingas verslo poreikiams, t. y. tikslui, kurio siekiama tvarkant Asmens duomenis.

8.7.2. Prieš pradedant tvarkyti Asmens duomenis teisėto intereso pagrindu, visada turi būti įvertintas konkretus

effect prior to giving consent. It shall be as easy to withdraw as to give consent.

8.3. **Contractual performance as the legal basis for Personal Data Processing**

8.3.1. The performance of a contract or pre-contractual steps may constitute a lawful basis for Personal Data Processing on condition that Personal Data being so processed are necessary for the pre-contractual steps or for the performance of the contract with Data Subject.

8.3.2. The performance of a contract or pre-contractual steps may constitute a lawful basis for Personal Data Processing on condition that both Data Subject and Group Company are (will be) the parties to the contract.

8.4. **Legal obligation as the legal basis for Personal Data Processing**

8.4.1. Group Companies shall process Personal Data seeking to fulfil their obligations imposed by Applicable Laws, including, but not limited to, obligations in employment law and social security areas.

8.4.2. Purposes, scope, time limits, and other terms and conditions of Personal Data Processing shall be set out in Applicable Laws.

8.4.3. A legal obligation may constitute a lawful basis for Personal Data Processing only if Personal Data Processing is explicitly (not obscurely) prescribed by Applicable Laws.

8.5. **Vital interests as the legal basis for Personal Data Processing**

8.5.1. Personal Data Processing shall be necessary in order to protect vital interests. A person's consent cannot constitute the basis for Personal Data Processing on the said basis.

8.6. **A task in public interest or performance of public functions**

8.6.1. Personal Data Processing on the basis that such processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Group Company in its capacity as Controller shall be permitted only in cases prescribed by Applicable Laws.

8.7. **Legitimate interest as the legal basis for Personal Data Processing**

8.7.1. Where Personal Data Processing is carried out by Group Company on the basis of legitimate interest, the purpose of such processing must be legitimate, and the processing methods or technologies must be the ones necessary for achieving Group Company's interests. Personal Data Processing must also be proportionate to the business needs, i.e. the purpose it is meant to address.

8.7.2. Personal Data Processing on the basis of legitimate interest shall always require the assessment

teisėtas interesas. Teisėto intereso vertinimo pagalba nustatomas Asmens duomenų tvarkymo tikslas, jo teisėtumas, Asmens duomenų tvarkymo priemonės bei metodai, o taip pat yra įvertinamas poveikis Duomenų subjektui, jo teisėms. Kaip turi būti atliktas teisėto intereso vertinimo testas, yra nurodyta Grupės Teisėto intereso įvertinimo procedūroje, kurią tvirtina Valdymo įmonė. Duomenų apsaugos pareigūnas yra atsakingas už teisėto intereso vertinimo atlikimą kiekvienos Asmens duomenų tvarkymo operacijos atžvilgiu, kai Asmens duomenys tvarkomi teisėto intereso pagrindu.

of the specific legitimate interest. By assessing the legitimate interest, the purpose, lawfulness, measures and methods of Personal Data Processing shall be determined, and the impact on Data Subject and on Data Subject's rights shall be identified. Instructions of how to conduct the assessment of legitimate interest shall be provided for in the Group's Procedure for the Assessment of Legitimate Interest approved by Management Company. Where Personal Data Processing is made on the basis of legitimate interest, the assessment of legitimate interest in respect of each Personal Data Processing operation shall be the responsibility of DPO.

9. ASMENS DUOMENŲ TVARKYMO TERMINAI IR ASMENS DUOMENŲ SAUGOJIMAS

9.1. Grupė ir Grupės įmonės tvarko Asmens duomenis vadovaudamosi Taikytinuose teisės aktuose ir Duomenų tvarkymo veiklos įrašuose nustatytais terminais, atsižvelgdamos į Asmens duomenų tvarkymo tikslus. Jei yra prieštaravimų tarp Taikytinų teisės aktų reikalavimų ir Duomenų tvarkymo veiklos įrašų, privaloma vadovautis Duomenų tvarkymo veiklos įrašais.

9.2. Pasibaigus nustatytam Asmens duomenų tvarkymo terminui, Asmens duomenys sunaikinami šių Taisyklių nustatyta tvarka. Taip pat Asmens duomenys nedelsiant yra sunaikinami, jeigu Duomenų subjektas Taikytinų teisės aktų nustatytais atvejais paprašo ištrinti jo Asmens duomenis (teisė būti pamirštam) ar nesutinka su Asmens duomenų tvarkymu ir Grupės įmonė neturi kito teisėto pagrindo Asmens duomenų tvarkymui arba Grupės įmonė turi pagrįstą įtarimą manyti, kad reikia užkirsti kelią neteisėtam Asmens duomenų naudojimui.

9.3. Asmens duomenys Grupės įmonės vadovo sprendimu gali būti saugomi ilgesnį terminą Taikytinų teisės aktų nustatyta tvarka ir sąlygomis, pavyzdžiui, jei yra pagrindo manyti, kad Asmens duomenų gali prireikti tiriant Grupės įmonės patalpose ar pastate, kuriame yra patalpos, įvykdytą nusikalstamą veiką, ar kitokį incidentą. Tokiu atveju Asmens duomenys saugomi iki bus priimtas atitinkamas teisėsaugos institucijų ar teismo sprendimas, susijęs su nusikalstama veika, ar kitoks asmenų, tiriančių/nagrinėjančių incidentą (pavyzdžiui, stichinių nelaimių atveju – draudikų), ar kitų asmenų, tiriančių/nagrinėjančių Grupės įmonei žalą sukėlusį įvykį, sprendimas ar išvada.

9.4. Popieriniai dokumentai sunaikinami tokiu būdu, kad būtų išlaikytas konfidencialumo principas. Konfidencialūs įrašai turėtų būti dedami į konfidencialias šiukšlių dėžes arba dedami į konfidencialius maišus, kuriuos surenka specialias dokumentų naikinimo paslaugas teikiančios įmonės.

9.5. Elektroninių įrašų ištrynimą prižiūri Duomenų apsaugos pareigūnas, jei reikia, pasitelkdamas IT saugos specialisto pagalbą. Bet kokia sunaikinimui skirta kompiuterinė įranga taip pat turėtų būti sunaikinama su IT saugos specialisto priežiūra, siekiant užtikrinti, kad visos laikmenos būtų fiziškai sunaikintos.

9. TIME LIMITS FOR PERSONAL DATA PROCESSING AND PERSONAL DATA STORAGE

9.1. Personal Data Processing by Group and Group Companies shall comply with time limits established in Applicable Laws and in Records of Processing Activities according to the purposes of Personal Data Processing. In the event of any discrepancies between Applicable Laws and Records of Processing Activities, Records of Processing Activities shall prevail.

9.2. After the expiry of established time limit for Personal Data Processing, Personal Data shall be destroyed pursuant to the procedure provided for in these Rules. Personal Data shall also be immediately destroyed if Data Subject requests that their Personal Data be erased ('right to be forgotten') in cases determined by Applicable Laws or if she/he objects to Personal Data Processing and Group Company has no other lawful basis for Personal Data Processing or if Group Company has reasonable grounds to believe that the unlawful use of Personal Data must be prevented.

9.3. By decision of Group Company's CEO, Personal Data may be stored for a longer period of time pursuant to the procedure and conditions determined by Applicable Laws, in cases where, for example, there are grounds to believe that Personal Data may be required for the investigation of a criminal offence or other incident conducted on the premises of Group Company or in the building where the premises are situated. In such a case, Personal Data shall be stored until a respective judgment with regard to the criminal offence is passed by law enforcement bodies or by court, or any other decision or conclusion is made by persons who investigate/analyse the incident (for example, by insurers in case of natural disasters) or by those who investigate/analyse the event that has caused damage to Group Company.

9.4. Paper documents shall be destroyed in a manner that ensures confidentiality principle. Confidential records shall be deposited in confidential waste bins or in confidential waste bags to be collected by companies providing specialised confidential waste disposal services.

9.5. Deletion of electronic records shall be supervised by Data Protection Officer who may involve an IT-Security Officer if needed. Any hardware intended for destruction shall be destroyed under the supervision of IT-Security Officer to ensure that all mediums are physically destroyed.

10. ATSKIRI ASMENS DUOMENŲ TVARKYMO ATVEJAI

10.1. **Asmens duomenų tvarkymas potencialių ar esamų klientų kreditingumo vertinimo tikslu**

10.1.1. Darbuotojas, prieš pradėdamas vertinti, ar Duomenų subjektui galima parduoti prekes ar paslaugas su atidėtu atsiskaitymo terminu (mokėjimu) ar kitaip vertinti asmens kreditingumą, turi gauti Duomenų subjekto prašymą sudaryti sutartį, kuris rengiamas pagal Grupės įmonės patvirtintą formą. Šiuo atveju Asmens duomenys tvarkomi vadovaujantis Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalies (b) punktu, t. y., siekiant imtis veiksmų kliento prašymu prieš sudarant sutartį.

10.1.2. Duomenų subjektui turi būti pateikta informacija, kaip Grupės įmonė tvarkys jo Asmens duomenis, pateikiama nuoroda į Grupės įmonės Privatumo politiką.

10.1.3. Atliekant Duomenų subjekto kreditingumo vertinimą, galima rinkti tik tiek Asmens duomenų apie Duomenų subjektą, kiek nurodoma Grupės įmonės kreditavimo rizikos valdymo taisyklėse.

10.2. **Asmens duomenų tvarkymas tiesioginės rinkodaros tikslu**

10.2.1. Darbuotojas, kuris tiesiogiai bendrauja su klientais ir teikia jiems pasiūlymus, organizuoja renginius ir šventes klientams, Darbuotojams ar jų vaikams, taip pat naudoja asmenų nuotraukas / filmuotą medžiagą, tvarko socialinių tinklų paskyras, t. y., pardavimo vadybininkas, administratorius, marketingo specialistas, personalo skyriaus darbuotojas ir kt., turi susipažinti su Atmintine darbuotojams dėl tiesioginės rinkodaros, renginių ir nuotraukų bei vaizdo įrašų (Atmintinės pridedamos kaip 3 priedas prie Taisyklių).

10.2.2. Naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu leidžiama tik Atmintinėje darbuotojams dėl tiesioginės rinkodaros, renginių ir nuotraukų bei vaizdo įrašų numatytais atvejais ir tvarka (Atmintinės pridedamos kaip 3 priedas prie Taisyklių).

10.2.3. Bet kokia komunikacija (pvz., elektroninio laiško siuntimas, skambinimas), siekiant gauti sutikimą teikti tiesioginės rinkodaros pasiūlymus, yra negalima komunikacijos metu neturint Duomenų subjekto sutikimo. Draudžiama siųsti elektroninius laiškus, SMS žinutes ar skambinti Duomenų subjektui klausiant, ar jis sutinka gauti tiesioginės rinkodaros pasiūlymus. Duomenų subjekto išankstinis sutikimas dėl Asmens duomenų naudojimo tiesioginės rinkodaros tikslais turi būti gaunamas kitais būdais (pvz., išreiškiant sutikimą interneto svetainėje (jei tokia forma naudojama), sudarant sutartį, užpildant įvairias formas).

10.2.4. Jeigu Asmens duomenys tvarkomi tiesioginės rinkodaros tikslais, Duomenų subjektas turi teisę nesutikti su tokiu duomenų tvarkymu, o jį davęs, bet kada nemokamai atšaukti, nesvarbu, ar tai yra pirminis ar tolesnis duomenų

10. INDIVIDUAL CASES OF PERSONAL DATA PROCESSING

10.1. **Personal Data Processing for assessment of the creditworthiness of potential or existing clients**

10.1.1. Before starting to assess whether goods or services may be sold to Data Subject under the deferred payment scheme or otherwise assess a person's creditworthiness, Employee must receive Data Subject's request for an agreement, such request to be made in the form approved by Management Company. In that case, Personal Data shall be processed in accordance with Article 6(1)(b) of General Data Protection Regulation, i.e. in order to take steps at the client's request prior to entering into a contract.

10.1.2. Data Subject must be provided with information on how his/her Personal Data will be processed by Group Company via reference to Group Company's Privacy Policy.

10.1.3. For assessing Data Subject's creditworthiness, Personal Data of that Data Subject may be collected only to the extent specified in Group Company's Credit Risk Management Rules.

10.2. **Personal Data Processing for direct marketing purposes**

10.2.1. Employee who directly communicates with clients and gives them offers or organizes events and celebrations for clients or Employees/their children or uses personal images/videos or manages social network accounts, i.e. a sales manager, an administrator, a marketing specialist, a personnel department employee, etc., must be familiar with the Memo to Employees on Direct Marketing, Events, Images and Videos (Memos attached as Annex 3 to the Rules).

10.2.2. Use of electronic communication services, including sending emails for direct marketing purposes shall only be permitted in cases and following procedure provided in the Memo to Employees on Direct Marketing, Events, Images and Videos (Memos attached as Annex 3 to the Rules).

10.2.3. No communication (e.g. sending an email letter or giving a call) in order to obtain consent to receiving direct marketing offers shall be permitted without Data Subject giving his/her consent to such communication. It shall not be allowed to send email letters, SMS messages or give calls to Data Subject asking whether he/she consents to receiving direct marketing offers. Data Subject's prior consent for the use of Personal Data for direct marketing purposes must be obtained in some other ways (e.g. by expressing such consent on the Internet website (should that form of consenting be used) or by making an agreement or by filling out certain forms).

10.2.4. Where Personal Data are processed for direct marketing purposes, Data Subject should have the right not to consent to such processing or, if already consented, to withdraw such consent at any time and free of charge, whether with regard to initial or further

tvarkymas. Apie tokią teisę Duomenų subjektas turi būti aiškiai informuojamas.

10.2.5. Grupės įmonė, gavusi Duomenų subjekto sutikimo atšaukimą arba nesutikimą tvarkyti Asmens duomenis, nedelsiant ištrina Duomenų subjekto Asmens duomenis ir nebesiunčia tiesioginės rinkodaros pranešimų. Šios teisės įgyvendinimas ribojamas, jei Asmens duomenų tvarkymas yra būtinas siekiant laikytis Taikytinų teisės aktų nustatytos teisinės prievolės ir (ar) siekiant pareikšti, vykdyti arba apginti teisėtus interesus. Bet kuriuo atveju, sutikimo atšaukimas ir/arba nesutikimas tvarkyti Asmens duomenis nedarys poveikio Asmens duomenų tvarkymo, atlikto iki atšaukimo, teisėtumui (t. y. Duomenų subjektui atšaukus sutikimą, neturi būti ištrinti iki tol teisėtai rinkti ar kitaip tvarkyti Asmens duomenys).

10.3. **Vaizdo duomenų tvarkymas**

10.3.1. Tvarkyti vaizdo duomenis (įrengti filmavimo kameras) galima tik jeigu tam yra teisėtas Bendrojo duomenų apsaugos reglamento 6 straipsnio 1 dalyje nurodytas pagrindas, pavyzdžiui, teisėtas interesas užtikrinti asmenų ir turto saugumą (BDAR 6 straipsnio 1 dalies f punktas).

10.3.2. Prieš patenkant į patalpas, kur įrengtos filmavimo kameros, privalo būti ženklai, informuojantys apie vykdomą vaizdo stebėjimą. Informaciniame ženkle privaloma nurodyti: (a) Asmens duomenų tvarkymo tikslą; (b) kontaktinę informaciją apie duomenų valdytoją (Grupės įmonę); (c) informaciją apie Duomenų subjekto teises arba nuorodą į Grupės įmonės Privatumo politiką.

10.3.3. Jeigu vaizdo kameras ketinama įrengti patalpoje, kur bus stebimi Darbuotojai, ar ketinama naudoti vaizdo kameras su garso įrašymo funkcija, prieš tai privaloma atlikti poveikio duomenų apsaugai vertinimą Taisyklių 13 dalyje numatyta tvarka.

10.3.4. Darbuotojai apie atliekamą vaizdo stebėjimą privalo būti informuoti šių Taisyklių 11 dalyje nurodyta tvarka.

10.4. **Darbuotojų Asmens duomenų tvarkymas**

10.4.1. Grupė, siekdama užtikrinti Darbuotojų Asmens duomenų apsaugą, nustato šiuos draudimus, taikomus visoms Grupės įmonėms:

(a) tvarkyti su darbo reikmėmis nesusijusius (perteklinius) Darbuotojo Asmens duomenis;

(b) pateikti Darbuotojo Asmens duomenis Tretiesiems asmenims, išskyrus Duomenų tvarkymo veiklos įrašuose ir (ar) Taikytinuose teisės aktuose nustatytus atvejus;

(c) pažeisti Darbuotojo asmeninio sužinojimo slaptumą, net ir įgyvendinant nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir komunikacines technologijas;

(d) daryti vaizdo ir garso įrašą, jei tiesiogiai siekiama kontroliuoti Darbuotojo darbo kokybę ir apimtis.

processing. That right should be explicitly brought to the attention of Data Subject.

10.2.5. In case of withdrawal of Data Subject's consent or objection by Data Subject to Personal Data processing, Group Company shall immediately delete Data Subject's Personal Data and discontinue sending direct marketing communications. This right shall be limited should Personal Data processing be necessary in order to comply with legal obligations under Applicable Laws and/or to establish, exercise and defend legal claims. Anyway, the withdrawal of consent and/or objection to Personal Data processing shall not affect the lawfulness of processing based on consent before its withdrawal (i.e. no Personal Data lawfully collected or otherwise processed before the withdrawal of Data Subject's consent shall be deleted).

10.3. **Processing of video data**

10.3.1. Processing of video data (installation of video cameras) shall only be permitted on legitimate grounds specified in Article 6(1) of General Data Protection Regulation, e.g., the legitimate interest to ensure the safety of people and property (Article 6(1)(f) of GDPR).

10.3.2. Entrance to the premises containing video cameras must be marked with signs warning about video surveillance. Such information signs must specify: (a) purpose for which Personal Data are processed; (b) Controller's (Group Company's) contact details (c) information about Data Subject's rights or reference given to Group Company's Privacy Policy.

10.3.3. A data protection impact assessment must be carried out in accordance with Section 13 of the Rules before video cameras are to be installed on the premises for watching Employees or video cameras with sound recording are intended to be used.

10.3.4. Information about video surveillance must be brought to the attention of Employees pursuant to Section 11 of these Rules.

10.4. **Processing of Employees' Personal Data**

10.4.1. To ensure the protection of Employees' Personal Data, the following bans applicable to all Group Companies have been established by Group:

(a) processing of Employee's Personal Data not related to work activities (excess data);

(b) provision of Employee's Personal Data to Third Parties except for the cases indicated in the Records of Processing Activities and/or Applicable Laws;

(c) breach of confidentiality of Employee's personal knowledge even when exercising ownership or possession rights to the information and communication technologies used at the workplace;

(d) video and audio recording carried out for direct control of Employee's work quality and scope.

10.4.2. Įgyvendindama Darbuotojų teisę į jų Asmens duomenų apsaugą, Grupė numato ir papildomus reikalavimus, taikomus kiekvienai Grupės įmonei:

(a) Valdymo įmonė parengia, reguliariai peržiūri ir, esant poreikiui, atnaujina: (i) Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašą, taikomą visai Grupei ir kiekvienai Grupės įmonei; (ii) Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašą. Kiekviena Grupės įmonė supažindina su šiais dokumentais savo Darbuotojus.

(b) Kiekviena Grupės įmonė parengia, reguliariai peržiūri ir, esant poreikiui, atnaujina Darbuotojų asmens duomenų saugojimo politiką bei supažindina su šiais dokumentais savo Darbuotojus.

(c) Grupei ar Grupės įmonei diegiant naujus technologinius procesus ir kitas Darbuotojų privataus gyvenimo apsaugą galinčias pažeisti priemones, privaloma surengti informavimo ir konsultavimo procedūras su Grupės įmonės darbo taryba (jeigu taikytina) ir, esant poreikiui, atlikti poveikio duomenų apsaugai vertinimą Taisyklių 13 dalyje numatyta tvarka.

10.4.3. Grupės įmonės elektroninės komunikacijos stebėjimą vykdo tik tais atvejais, kai toks Darbuotojo elektroninės komunikacijos stebėjimas yra būtinas ir negalima imtis kitokių prevencinių priemonių, kurios mažiau ribotų asmenų privatumą.

10.4.4. Esant išankstiniam Darbuotojo sutikimui, Grupės įmonė taip pat gali tvarkyti kitus tokio Darbuotojo Asmens duomenis. Tais atvejais, kai sutikimas yra vienintelis teisinis pagrindas, kuriuo vadovaujantis galima tvarkyti Darbuotojo Asmens duomenis, Darbuotojas turi teisę bet kada atšaukti savo sutikimą šių Taisyklių nustatyta tvarka ir (ar) įgyvendinti kitas savo, kaip Duomenų subjekto teises, numatytas Taikytinuose teisės aktuose.

10.4.5. Detali informacija apie Darbuotojų asmens duomenų tvarkymą yra pateikiama Darbuotojų asmens duomenų saugojimo politikoje. Informacija apie Darbuotojų stebėseną yra pateikiama Grupės Informacinių technologijų ir darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkoje.

10.5. **Kandidatų asmens duomenų tvarkymas**

10.5.1. Grupės įmonė turi teisę tvarkyti tik tuos Kandidato Asmens duomenis, kurie susiję su šio asmens kvalifikacija, profesiniais gebėjimais ir dalykinėmis savybėmis, išskyrus įstatymuose nurodytus atvejus.

10.5.2. Draudžiama tvarkyti Kandidato Specialių kategorijų asmens duomenis bei Asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas arba susijusias saugumo priemones, išskyrus tuos atvejus, kai šie Asmens duomenys būtini patikrinti, ar Kandidatas

10.4.2. To implement Employees' right to the protection of their Personal Data, Group shall also determine additional requirements applicable to each Group Company:

(a) Management Company shall draft, review on a regular basis and, where applicable, update (i) the Procedure for the Use of Information and Communication Technologies and for Monitoring and Control of Employees at Their Workplace; (ii) the Procedure for Responding to Personal Data Breaches. Each Group Company shall bring the above documents to the attention of its Employees.

(b) Each Group Company shall draft, review on a regular basis and, where applicable, update the Policy for the Storage of Employees' Personal Data and shall bring it to the attention of its Employees.

(c) When implementing new technological processes or other measures that are likely to breach Employees' private life, the Group or Group Company shall organise information and consultation procedures concertedly with Group Company's works council (if any) and, where necessary, perform a data protection impact assessment in accordance with Section 13 of the Rules.

10.4.3. Group Companies shall carry out electronic communication monitoring only when such monitoring of Employee's electronic communication is necessary and no other preventative measures less restricting the privacy of persons are available.

10.4.4. Group Company shall also be allowed to process Employee's other Personal Data subject to that Employee's prior consent. Where such consent constitutes the only legal basis for the processing of Employee's Personal Data, Employee shall be entitled to withdraw his/her consent at any time in accordance with these Rules and/or to exercise his/her other rights, to which Employee is entitled in his/her capacity as Data Subject, as determined in Applicable Laws.

10.4.5. Details on the processing of Employees' Personal Data are provided in the Policy for the Storage of Employees' Personal Data. Information on employee monitoring is given in the Procedure for the Use of Information and Communication Technologies and for Monitoring and Control of Employees at Their Workplace.

10.5. **Processing of Candidates' Personal Data**

10.5.1. Only Candidate's Personal Data relating to that person's qualifications, professional skills and business qualities may be processed by Group Company unless otherwise required by law.

10.5.2. It shall not be allowed to process Special Categories of Candidate's Personal Data or Personal Data relating to criminal convictions and offences, or to security measures unless such Personal Data must be checked to ensure whether Candidate concerned

atitinka įstatymuose nustatytus reikalavimus pareigoms eiti arba darbams dirbti.

10.5.3. Grupės įmonė gali rinkti Kandidato Asmens duomenis, susijusius su kvalifikacija, profesiniais gebėjimais ir dalykinėmis savybėmis, iš buvusio darbdavio prieš tai informavusi Kandidatą, o iš esamo darbdavio – tik Kandidato sutikimu. Informavimas gali būti pateikiamas pačiame darbo skelbime arba darant nuorodą į Grupės įmonės Privatumo politiką.

10.5.4. Grupės įmonė neturi teisės peržiūrėti Kandidatų socialinės žiniasklaidos tinklų asmeninių paskyrų, nebent apie tai iš anksto informuojama ir tik tiek, kiek tai būtina nustatyti Kandidato tinkamumą konkrečių funkcijų vykdymui. Socialinės paskyros, skirtos išimtinai asmeniniam interesui tenkinti, neturėtų būti tikrinamos.

10.5.5. Grupės įmonė neturi teisės reikalauti, kad Kandidatas leistų gauti informaciją, kuria Kandidatas su kitais dalijasi per socialinius tinklus.

10.5.6. Grupės įmonė privalo sunaikinti be galimybės atkurti visus Asmens duomenis, kurie susiję su Kandidatais į Grupės įmonės siūlomas darbo vietas, jei Kandidatui pasiūlymas įsidarbinti nebuvo pateiktas, taip pat, jei buvo pateiktas, o pasiūlymo buvo atsisakyta ir jei Kandidatas neišreiškė sutikimo, kad jo Asmens duomenys būtų tvarkomi su tikslu ateityje pasiūlyti jam darbo vietą, atitinkančią jo kvalifikaciją.

10.5.7. Skelbime dėl darbo vietos arba Kandidato Asmens duomenų gavimo metu (jei atranka vykdoma ne skelbimo būdu) privalo būti pateikta visa Bendrojo duomenų apsaugos reglamento 13 arba 14 straipsnyje nurodyta informacija (santrauka pateikiama Taisyklių 2 priede) arba pateikta nuoroda į Privatumo politiką ir informacija, kad bus kreipiamasi į buvusius darbdavius, ir (arba) bus tikrinama Kandidato paskyra profesiniame socialinės žiniasklaidos tinkle (jeigu taikoma). Jeigu norima pasilikti Kandidato CV ir (arba) motyvacinį laišką, Kandidatui pasiūloma pasirašyti Kandidato sutikimą dėl Asmens duomenų tvarkymo, kurio formą tvirtina Valdymo įmonė.

10.6. **Asmens duomenų tvarkymas interneto svetainėse, socialinės žiniasklaidos paskyrose**

10.6.1. Informaciją, kuri yra susijusi su Asmens duomenų rinkimu, naudojimu, susipažinimu, tvarkymu, Asmens duomenų tvarkymo mastu, kiekviena Grupės įmonė pateikia Duomenų subjektams savo Privatumo politikoje.

10.6.2. Grupės įmonė, skelbdama Darbuotojų Asmens duomenis savo interneto svetainėje (išskyrus kontaktinių duomenų skelbimą) ar socialinės žiniasklaidos paskyrose, privalo gauti tokių Darbuotojų išankstinius sutikimus.

10.7. **Specialių kategorijų Asmens duomenų tvarkymas**

10.7.1. Grupės įmonės neturi teisės tvarkyti Specialių kategorijų asmens duomenų, išskyrus atvejus, kai:

(a) Duomenų subjektas aiškiai sutiko, kad tokie Asmens duomenys būtų tvarkomi vienu ar keliais nurodytais

satisfies the statutory requirements that make him/her suitable for the office or the job.

10.5.3. Group Company may collect Candidate's Personal Data relating to his/her qualifications, professional skills and business qualities from a former employer with prior notice to Candidate, and from the current employer – only with Candidate's consent. Notification may be given in the job advertisement or by reference to Privacy Policy of the Group Company.

10.5.4. Group Company shall have no right to view Candidates' personal accounts in social media networks otherwise than with prior notice to Candidate and only to the extent necessary to determine Candidate's suitability for certain job responsibilities. No social media accounts used solely for personal needs should be checked.

10.5.5. Group Company shall have no right to demand from Candidate to allow access to information shared by Candidate with others via social networks.

10.5.6. Group Company must destroy by a permanent deletion all Personal Data of Candidates applying to positions offered by Group Company if no employment offer has been issued to Candidate or, if issued, the offer has been declined and Candidate has not given consent to the processing of his/her Personal Data for the purpose of offering him/her another position corresponding to Candidate's qualifications in the future.

10.5.7. All information indicated in Article 13 or Article 14 of GDPR (summary provided in Annex 2 to the Rules) or reference to Privacy Policy as well as information that former employers will be contacted and/or that Candidate's account on the professional social media site (if any) will be checked must be given in the job advertisement or at the time of receiving Candidate's Personal Data (if the selection is carried out otherwise than through job advertisements). Should Candidate's CV and/or motivation letter be wished to be retained, Candidate shall be offered to sign Candidate's Consent to the Processing of Personal Data Form approved by Management Company.

10.6. **Processing of Personal Data on Internet websites and in social media accounts**

10.6.1. Information relating to the collection, use, processing of and access to Personal Data as well as the scope of such processing shall be made available by each Group Company to Data Subjects in its Privacy Policy.

10.6.2. For publishing Employees' Personal Data on its website (except for contact data) or in social media accounts, Group Company must obtain prior consents of those Employees.

10.7. **Processing of Special Categories of Personal Data**

10.7.1. Group Company shall not be entitled to process Special Categories of Personal Data, except when:

(a) Data Subject has given his/her explicit consent to the processing of such Personal Data for one or

tikslais, išskyrus Taikytinuose teisės aktuose numatytas išimtis;

(b) tvarkyti Specialių kategorijų asmens duomenis būtina, kad Grupės įmonė arba Duomenų subjektas galėtų įvykdyti prievoles ir naudotis specialiomis teisėmis darbo ir socialinės apsaugos teisės srityje;

(c) tvarkyti Specialių kategorijų asmens duomenis būtina, kad būtų apsaugoti gyvybiniai Duomenų subjekto arba kito fizinio asmens interesai, kai Duomenų subjektas dėl fizinių ar teisinių priežasčių negali duoti sutikimo;

(d) tvarkomi Asmens duomenys, kuriuos Duomenų subjektas yra akivaizdžiai paskelbęs viešai;

(e) tvarkyti Specialių kategorijų asmens duomenis būtina siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus;

(f) tvarkyti Specialių kategorijų asmens duomenis būtina dėl svarbaus viešojo intereso priežasčių;

(g) tvarkyti Specialių kategorijų asmens duomenis būtina dėl viešojo intereso priežasčių visuomenės sveikatos srityje, siekiant užtikrinti aukštus sveikatos priežiūros standartus.

10.7.2. Specialių kategorijų asmens duomenys turi būti šifruojami.

10.8. **Asmens duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas**

10.8.1. Grupės įmonėms draudžiama tvarkyti asmens duomenis apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas, išskyrus atvejus, kai tai aiškiai leidžiama Taikytinuose teisės aktuose.

10.9. **Asmens duomenų tvarkymas Grupės įmonės teisių ir interesų apsaugos įgyvendinimui**

10.9.1. Grupės įmonė, siekdama apsaugoti savo interesus, gali Asmens duomenis perduoti teismui, antstoliui, Grupei ar Grupės įmonei atstovaujantiems teisininkams, antstoliams ar kitiems Grupės ar Grupės įmonės interesams atstovaujantiems asmenims.

11. DARBUOTOJŲ SUPAŽINDINIMAS

11.1. Kai pagal Bendrojo duomenų apsaugos reglamento, kitų Taikytinų teisės aktų, šių Taisyklių ar kitų vidinių Grupės ar Grupės įmonių dokumentų reikalavimus Darbuotojai turi būti supažindinami su dokumentais, reglamentuojančiais Asmens duomenų apsaugą, Darbuotojai supažindinami taip:

11.1.1. nedelsiant po atitinkamo dokumento patvirtinimo jis išsiunčiamas Darbuotojams, kurie turi Grupės ar Grupės įmonės jiems suteiktą elektroninio pašto adresą, tokiu elektroninio pašto adresu, ar kitu elektroninio pašto adresu, kurį Grupės įmonė teisėtai tvarko ar kitomis Grupėje ar Grupės įmonėje paprastai naudojamomis elektroninėmis Darbuotojų informavimo priemonėmis;

more specified purposes unless otherwise provided for in Applicable Laws;

(b) processing of Special Categories of Personal Data is necessary for Group Company or Data Subject to carry out their obligations and to exercise specific rights in the field of labour and social security law;

(c) processing of Special Categories of Personal Data is necessary for protecting the vital interests of Data Subject/any other natural person in cases when Data Subject is physically or legally incapable of giving consent;

(d) processing relates to Personal Data that have been manifestly made public by Data Subject;

(e) processing of Special Categories of Personal Data is necessary for the establishment, exercise or defence of legal claims;

(f) processing of Special Categories of Personal Data is necessary for the reasons of substantial public interest;

(g) processing of Special Categories of Personal Data is necessary for the reasons of public interest in the field of public health seeking to ensure high standards of health care.

10.7.2. Special Categories of Personal Data must be encrypted.

10.8. **Processing of Personal Data relating to criminal convictions and offences**

10.8.1. Group Companies shall be prohibited from the processing of Personal Data relating to criminal convictions and offences, except when explicitly permitted by Applicable Laws.

10.9. **Personal Data processing for implementing protection of Group Company's rights and interests**

10.9.1. In order to protect its interests, Group Company may transfer Personal Data to a court/bailiff or to lawyers/bailiffs representing Group or Group Company or to other persons representing Group's or Group Company's interests.

11. EMPLOYEE AWARENESS

11.1. If according to General Data Protection Regulation, other Applicable Laws, these Rules or other internal documents of Group/Group Company, Employees must be familiarized with the documents governing Personal Data protection, such documents shall be made available to them as follows:

11.1.1. when approved, a relevant document shall be immediately forwarded to Employees who have an email address assigned to them by Group or Group Company at such email address assigned to them or at any other email address lawfully managed by Group Company or by other electronic means normally used by the Group or

Group Company for the purposes of informing the Employees;

11.1.2. nedelsiant po atitinkamo dokumento patvirtinimo jis patalpinamas Grupės ar Grupės įmonės serveryje (ar kitoje vietoje, kur saugomi visi Grupės ar Grupės įmonės vidaus dokumentai, tvarkos ir taisyklės) ir ten yra pasiekiamas Darbuotojams bet kuriuo metu;

11.1.2. when approved, a relevant document shall be immediately uploaded onto Group's or Group Company's server (or elsewhere, where all internal documents, procedures and rules of Group or Group Company are stored) to be accessible to Employees at any time;

11.1.3. kiekvienas naujas Darbuotojas supažindinamas su tokiu dokumentu pirmąją jo darbo ar funkcijų atlikimo dieną Grupėje ar Grupės įmonėje, pateikiant jam dokumentą elektroniniu paštu ar kitaip sudarant galimybę pasiekti dokumentą;

11.1.3. each new Employee shall be made familiar with such document on the first day of his/her employment or engagement by Group or Group Company, by receiving that document via email or otherwise getting access to it;

11.1.4. kitais atvejais, kai dėl bet kokių priežasčių nėra galimybės Darbuotojo supažindinti elektroniniu paštu, su dokumentu supažindinami raštu.

11.1.4. however, where due to some reasons sending the document by email is not possible, Employee shall be granted access to it in hardcopy format.

11.2. Elektroniniu paštu išsiųstas dokumentas yra laikomas įteiktu:

11.2. A document sent by email shall be deemed to have been delivered:

11.2.1. tą pačią darbo dieną, jei buvo išsiųstas ne vėliau kaip likus 1 (vienai) valandai iki atitinkamo Darbuotojo darbo laiko pabaigos;

11.2.1. on the same business day if sent at least 1 (one) hour before end of the working day of the Employee;

11.2.2. kitą darbo dieną, jei buvo išsiųstas vėliau nei likus 1 (vienai) valandai iki atitinkamo Darbuotojo darbo laiko pabaigos arba po jo darbo laiko pabaigos;

11.2.2. on the next business day if sent less than 1 (one) hour before end of the working day of the Employee or thereafter;

11.2.3. artimiausią darbo dieną, jei buvo išsiųstas poilsio ar švenčių dieną;

11.2.3. on the immediately succeeding business day if sent on a day off or on a public holiday;

11.2.4. artimiausią Darbuotojo darbo dieną, jei buvo išsiųstas Darbuotojui jo kasmetinių atostogų ar nedarbingumo metu;

11.2.4. on the immediately succeeding business day of the Employee if sent to Employee during his/her annual leave or sick leave;

11.2.5. artimiausią Darbuotojo darbo dieną po komandiruotės, jei buvo išsiųstas Darbuotojui jo komandiruotės metu, o komandiruotėje nebuvo užtikrintas interneto ryšys.

11.2.5. on Employee's business day immediately succeeding his/her business trip if sent to Employee during such business trip on which no Internet service was available.

12. ASMENS DUOMENŲ PERDAVIMAS (TEIKIMAS)

12.1. Asmens duomenys gali būti perduodami (teikiami) kitiems asmenims tik Taikytinuose teisės aktuose numatytais atvejais ir tvarka.

12.2. Grupės įmonė Asmens duomenis gali perduoti į Trečiąsias valstybes tik laikydamasi Taikytinų teisės aktų reikalavimų, jei Trečioji valstybė užtikrina tinkamo lygio apsaugą, Grupės įmonės Duomenų tvarkymo veiklos įrašuose numatytais atvejais ir apimtimi.

12.3. Galimi Asmens duomenų perdavimo į Trečiąsias valstybes pagrindai:

12.3.1. Perduodant Asmens duomenis į Trečiąsias valstybes, reikia įsitikinti, ar tokia Trečioji valstybė suteikia tinkamą Asmens duomenų apsaugos lygį pagal Europos Komisijos sprendimą. Trečiųjų šalių sąrašas, kurios užtikrina tinkamą apsaugos lygį yra skelbiamas čia.

12. TRANSFER (SUBMISSION) OF PERSONAL DATA

12.1. Personal Data may only be transferred (submitted) to others when and as required by Applicable Laws.

12.2. Group Company shall be permitted to transfer Personal Data to Third Countries strictly in accordance with Applicable Laws provided that Third Country ensures an adequate level of protection in the cases and to the extent determined in Group Company's Records of Processing Activities.

12.3. It shall be possible to transfer Personal Data to Third Countries on the following grounds:

12.3.1. When transferring Personal Data to Third Countries, it should be ascertained whether that Third Country ensures adequate level of protection in accordance with a decision of the European Commission. A list of Third Countries ensuring adequate level of protection can be accessed here.

12.3.2. Jeigu Trečioji valstybė nėra tinkamą Asmens duomenų apsaugą užtikrinančių šalių sąraše, tuomet Grupės įmonė gali perduoti Asmens duomenis į Trečiąją valstybę pagal Bendrojo duomenų apsaugos reglamento V skyriaus nuostatas, pavyzdžiui:

a) Grupės įmonė su Trečiąja valstybe gali pasirašyti standartines duomenų apsaugos sąlygas, kurios skelbiamos čia.

b) Asmens duomenų perdavimas yra būtinas Duomenų subjekto ir Grupės įmonės sutarčiai vykdyti.

13. POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

13.1. Poveikio duomenų apsaugai vertinimas Grupėje ar Grupės įmonėje atliekamas, kai dėl Asmens duomenų tvarkymo gali kilti didelis pavojus asmenų teisėms ir laisvėms.

13.2. Poveikio duomenų apsaugai vertinimas atliekamas pagal Valdymo įmonės patvirtintą formą. Poveikio duomenų apsaugai vertinimą atlieka atsakingu paskirtas darbuotojas, konsultuojamas ir prižiūrimas Duomenų apsaugos pareigūno.

13.3. Poveikio duomenų apsaugai vertinimas turi būti atliekamas prieš Asmens duomenų tvarkymą. Jeigu, atliekant poveikio duomenų apsaugai vertinimą, nustatoma, kad tvarkant Asmens duomenis kiltų didelis pavojus, jei Grupė ar Grupės įmonė nesiimtų priemonių pavojui sumažinti, Grupė ar Grupės įmonė, prieš pradėdama tvarkyti Asmens duomenis, konsultuojasi su Priežiūros institucija.

13.4. Panašius didelius pavojus keliančių Asmens duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą. Vienas bendras vertinimas gali būti atliekamas ir kelių Grupės įmonių Asmens duomenų tvarkymo operacijų atžvilgiu.

14. ASMENS DUOMENŲ SAUGUMO PRIEMONĖS

14.1. **Organizacinės ir techninės saugumo priemonės**

14.1.1. Siekdamos užtikrinti Asmens duomenų apsaugą, Grupė ir Grupės įmonės įgyvendina arba numato įgyvendinti organizacines, technines ir fizines priemones.

14.1.2. Be kitų priemonių, įgyvendinamos šios organizacinės Asmens duomenų saugumo priemonės:

(a) Valdymo įmonė patvirtina Informacinių ir komunikacinių technologijų naudojimo ir darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašą, kuris yra taikomas visoms Grupės įmonėms.

12.3.2. Where Third Country is not on the list of countries ensuring adequate Personal Data protection, then Group Company may transfer Personal Data to Third Country in accordance with Chapter V of General Data Protection Regulation, for example:

(a) Group Company and Third County may sign standard data protection rules, which can be accessed here.

(b) Personal Data transfer is necessary for carrying out the agreement between Data Subject and Group Company.

13. DATA PROTECTION IMPACT ASSESSMENT

13.1. A data protection impact assessment shall be performed in Group or Group Company when Personal Data processing is likely to result in a high risk to the rights and freedoms of natural persons.

13.2. The data protection impact assessment shall be performed in the form approved by Management Company. The data protection impact assessment shall be performed by a designated person under the advice and supervision of DPO.

13.3. The data protection impact assessment shall be performed prior to Personal Data processing. Where the data protection impact assessment indicates that the processing of Personal Data might result in a high risk if no measures to reduce it are taken by Group or Group Company, Group or Group Company shall consult the Supervisory Authority prior to the processing of Personal Data.

13.4. A single assessment may address a set of similar processing operations that present similar high risks. One common assessment may be performed with respect to Personal Data processing operations carried out by several Group Companies.

14. PERSONAL DATA SECURITY MEASURES

14.1. **Organisational and technical security measures**

14.1.1. Seeking to ensure Personal Data protection, Group and Group Companies shall implement/seek to implement organizational, technical and physical measures.

14.1.2. The following organizational Personal Data security measures shall be implemented apart from other measures:

(a) Management Company shall approve the Procedure for the Use of Information and Communication Technologies and for Monitoring and Control of Employees at their Workplace to be applied through Group.

(b) Valdymo įmonė patvirtina Poveikio duomenų apsaugai vertinimo procedūrą, kurią taiko visos Grupės įmonės.

(b) Management Company shall approve the Data Protection Impact Assessment Procedure to be applied throughout Group.

(c) Valdymo įmonė patvirtina Teisėto intereso vertinimo procedūrą, kurią taiko visos Grupės įmonės.

(c) Management Company shall approve the Legitimate Interest Assessment Procedure to be applied throughout Group.

(d) Kiekvienoje Grupės įmonėje Saugumo politikoje numatyta tvarka vedamas, peržiūrimas ir atnaujinamas IT išteklių, naudojamų Asmens duomenims tvarkyti, registras (techninės, programinės ir tinklo įrangos).

(d) Each Group Company shall maintain, review and update a register of IT resources used for Personal Data processing (hardware, software and network equipment) in accordance with the Security Policy.

(e) Visi Grupės ar atskiros Grupės įmonės IT sistemų pakeitimai stebimi ir registruojami Saugumo politikoje numatyta tvarka.

(e) All Group's or Group Company's IT system updates shall be monitored and recorded in accordance with the Security Policy.

(f) Valdymo įmonė patvirtina išsamią reagavimo į Asmens duomenų saugumo pažeidimus ir jų padarinių likvidavimo tvarką (Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašas), taikomą visoms Grupės įmonėms.

(f) a comprehensive Personal Data breach response and liquidation procedure shall be approved by Management Company (the Procedure for Responding to Personal Data Breaches) to be applied throughout Group.

(g) Valdymo įmonė tvirtina Grupei ir visoms Grupės įmonėms taikomą saugumo politiką.

(g) The Management Company approves the Security Policy applicable to the Group and Group Companies.

14.1.3. Grupėje taikomos techninės saugumo priemonės numatomos Saugumo politikoje.

14.1.3. The technical security measures applicable in the Group shall be determined in the Security Policy.

14.1.4. Be kitų priemonių įgyvendinamos šios fizinės saugumo priemonės:

14.1.4. Apart from other measures, the following physical security measures shall be implemented:

(a) Dokumentai, kuriuose yra Asmens duomenys, privalo būti laikomi rakinamuose balduose ar patalpose.

(a) documents containing Personal Data shall be kept in locked cabinets or premises;

(b) Privalo būti laikomasi „švaraus stalo" principo.

(b) the "clean table" principle shall be respected;

(c) Įgyvendinama Trečiųjų asmenų įėjimo kontrolė.

(c) Third Party entry access control shall be implemented.

14.2. **Reikalavimai asmenims, tvarkantiems Asmens duomenis**

14.2. **Requirements for persons processing Personal Data**

14.2.1. Prieiga prie Asmens duomenų gali būti suteikta tik tam Darbuotojui, kuriam Asmens duomenys yra reikalingi jo funkcijoms vykdyti. Darbuotojas automatiškai netenka teisės tvarkyti Asmens duomenų, kai pasibaigia darbo ar kiti teisiniai santykiai su Grupės įmone arba jo darbo ar kitos funkcijos pasikeičia tokiu būdu, kad prieiga prie Asmens duomenų jam tampa nebebūtina.

14.2.1. Access to Personal Data may only be granted to Employee who needs such Personal Data for the performance of his/her job responsibilities. Employee shall automatically forfeit the right to process Personal Data upon termination of his/her employment or other legal relationship with Group Company or change of his/her job or other responsibilities to such extent that access to Personal Data becomes unnecessary.

14.2.2. Su Asmens duomenimis galima atlikti tik tuos veiksmus, kuriems atlikti Darbuotojui yra suteiktos teisės.

14.2.2. Only authorised actions shall be permitted to be performed by Employee with Personal Data.

14.2.3. Darbuotojas, tvarkantis Asmens duomenis, privalo:

14.2.3. Employee processing Personal Data shall:

(a) Laikytis pagrindinių Asmens duomenų tvarkymo reikalavimų ir saugumo reikalavimų, įtvirtintų šiose Taisyklėse ir Taikytinuose teisės aktuose.

(a) comply with the main Personal Data processing requirements and security requirements established in these Rules and in Applicable Laws;

(b) Laikytis jam taikomo konfidencialumo susitarimo nuostatų.

(b) comply with the provisions of the relevant confidentiality agreement;

(c) Nepažeisti šiose Taisyklėse ir/ar Saugumo politikoje numatytų ir/ ar kitų Grupės ar Grupės įmonės nustatytų organizacinių ir techninių Asmens duomenų saugumo priemonių.

(d) Neatskleisti, neperduoti ir nesudaryti sąlygų bet kokiomis priemonėmis susipažinti su Asmens duomenimis nė vienam asmeniui, kuris nėra įgaliotas tvarkyti Asmens duomenų.

(e) Domėtis Asmens duomenų apsaugos aktualijomis ir problemomis, esant galimybei kelti kvalifikaciją asmens duomenų teisinės apsaugos srityje.

14.2.4. Tinkamo Asmens duomenų tvarkymo tikslais Grupė siekia užtikrinti Asmens duomenų tvarkymo mokymus visiems Darbuotojams, kurie tvarko Asmens duomenis, vykdydami savo tiesiogines funkcijas. Mokymai vykdomi ne rečiau kaip kartą per kalendorinius metus.

14.3. **Prieigos kontrolė**

14.3.1. Prieigos teisės prie Grupės ar atskiros Grupės įmonės informacinių sistemų, kuriose tvarkomi Asmens duomenys, nustatomos Saugos politikoje. Šios teisės yra nustatomos, atsižvelgiant į kiekvieno Darbuotojo pareigas, vykdomas funkcijas. IT saugos specialistas turi užtikrinti, kad Darbuotojai, kuriems suteiktas leidimas naudotis Grupės ar Grupės įmonės informacinėmis sistemomis, kuriose tvarkomi Asmens duomenys, turėtų prieigą tik prie tų Asmens duomenų, kuriems taikomas jų prieigos leidimas (prieigos duomenų kontrolė). Tais atvejais, kai būtina nukrypti nuo patvirtintų prieigos teisių taisyklių, arba reikia pavaduoti konkretų Darbuotoją, prieigos teises suteikia IT saugos specialistas, tiesioginio konkretaus Darbuotojo vadovo arba Grupės įmonės vadovo siūlymu, esant Duomenų apsaugos pareigūno pritarimui. IT saugos specialistas veda tokių prieigos teisių sąrašą.

14.3.2. Grupė ar Grupės įmonė, suteikdama prieigą prie informacijos, vadovaujasi šiais principais:

(a) būtinumo žinoti principas – leidimas susipažinti su informacija gali būti duodamas tik tais atvejais, kai tai yra būtina veiklai vykdyti;

(b) mažiausių privilegijų principas – naudotojams suteikti leidimai turi atitikti paskirtį, kuriai informacija bus naudojama; ir

(c) pareigų atskyrimo principas – sprendimai dėl prieigos teisių turi būti priimami atsižvelgiant į galimus interesų konfliktus.

14.4. **Asmens duomenų saugumo pažeidimas**

14.4.1. Duomenų apsaugos pareigūnas nuolat stebi Grupėje vykdomų Asmens duomenų tvarkymo procesų atitiktį Taisyklėms bei Taikytiniems teisės aktams.

14.4.2. Įvykus bet kokiam Asmens duomenų saugumo pažeidimui, dėl kurio Duomenų subjektas gali patirti kūno sužalojimą, turtinę ar neturtinę žalą, pavyzdžiui, prarasti savo Asmens duomenų kontrolę, patirti teisių apribojimą,

(c) refrain from breaching any organisational or technical Personal Data security measures provided for in these Rules and/or the Security Policy and/or other measures established by Group or Group Companies;

(d) refrain from disclosing, transferring or giving whatever other access to Personal Data to anyone not authorised to process Personal Data;

(e) take interest in Personal Data protection issues and problems, and, if possible, raise qualifications in the field of legal protection of Personal Data.

14.2.4. For the purpose of proper processing of Personal Data, Group shall seek to ensure Personal Data processing trainings to all Employees processing Personal Data in the course of their direct job responsibilities. Such trainings shall be organised at least once per calendar year.

14.3. **Access control**

14.3.1. Rights of access to Group's or Group Company's information systems used to process Personal Data shall be defined in the Security Policy. These rights shall be determined considering each Employee's duties and job responsibilities. IT-Security Officer shall ensure that Employees authorised to use Group's/Group Company's information systems used to process Personal Data may access such Personal Data only to the extent permitted by their access authorisation (access data control). In cases where derogation from the approved rules for access is necessary or substitution of some particular Employee is required, such access rights shall be granted by IT-Security Officer by suggestion from that Employee's immediate superior of from Group Company's CEO subject to DPO's approval. IT-Security Officer shall maintain a list of such access rights.

14.3.2. When providing access to information, Group or Group Company shall adhere to the following principles:

(a) the need-to-know principle – access to information may only be given when this is necessary for the performance of activities;

(b) the least privilege principle – authorisations granted to users must be consistent with the intended use of information; and

(c) the separation-of-duty principle – decisions on the access rights must be made with due regard to possible conflicts of interest.

14.4. **Personal Data security breaches**

14.4.1. DPO shall constantly monitor the compliance of Personal Data processing operations carried out in Group with these Rules and Applicable Laws.

14.4.2. In the event of any Personal Data breach, which may result in physical, pecuniary or non-pecuniary damage to Data Subject, such as loss of control over his/her Personal Data or limitation of his/her rights or

diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, pakenkta reputacijai, prarasti asmens duomenys, kurie saugomi profesine paslaptimi, konfidencialumas, padaryta kita ekonominė ar socialinė žala atitinkamam Duomenų subjektui, atitinkama Grupės įmonė privalo pranešti Priežiūros institucijai ir/ar pačiam Duomenų subjektui nepagrįstai nedelsdama ir, jei įmanoma, nuo to laiko, kai apie tai buvo sužinota, praėjus ne daugiau kaip 72 (septyniasdešimt dviem) valandoms, laikantis reikalavimų ir tvarkos, kuri yra numatyta Valdymo įmonės patvirtintame Asmens duomenų saugumo pažeidimų reagavimo tvarkos apraše, naudojant prie jo pridėtą pranešimo formą.

discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to relevant Data Subject, Group Company concerned shall notify Supervisory Authority and/or Data Subject concerned without undue delay and, where feasible, not later than 72 hours after having become aware of such breach, acting in accordance with the requirements and in the manner determined in the Procedure for Responding to Personal Data Breaches approved by Management Company and using the recommended notification form attached to the said Procedure for Responding to Personal Data Breaches.

15. DUOMENŲ SUBJEKTŲ TEISIŲ ĮGYVENDINIMAS

15.1. Duomenų subjektas turi teisę pasinaudoti visomis savo, kaip Asmens duomenų subjekto, teisėmis, pateikęs Grupės įmonei asmens tapatybę patvirtinantį dokumentą arba teisės aktų nustatyta tvarka ar elektroninių ryšių priemonėmis, kurios leidžia tinkamai identifikuoti asmenį, patvirtinęs savo asmens tapatybę.

15.2. Grupės įmonės užtikrina Duomenų subjektų teises vadovaujantis Bendrojo duomenų apsaugos reglamento III skyriaus nuostatomis, Duomenų subjektų teisių įgyvendinimo tvarkoje, Privatumo politikoje ir šiose Taisyklėse nustatyta tvarka, apimtimi ir terminais. Valdymo įmonė tvirtina Duomenų subjektų teisių įgyvendinimo tvarką ir ji privaloma visoms Grupės įmonėms.

15. IMPLEMENTATION OF DATA SUBJECTS' RIGHTS

15.1. Data Subject shall have the right to use all of the rights to which he/she is entitled as Data Subject after submission of an identity document or confirmation of his/her identity to Group Company in the manner determined by laws or via electronic communication means that allow for the proper identification of a person.

15.2. Group Companies shall ensure Data Subjects' rights in accordance with Chapter III of GDPR, the Procedure for the Implementation of Data Subjects' Rights, Privacy Policy, and these Rules. The Procedure for the Implementation of Data Subjects' Rights shall be approved by Management Company and shall binding on all Group Companies.

16. ATSAKOMYBĖ

16.1. Darbuotojams, tvarkantiems Asmens duomenis, Duomenų apsaugos pareigūnui, kurie pažeidžia Bendrajame duomenų apsaugos reglamente ar kituose Taikytinuose teisės aktuose numatytus reikalavimus arba šias Taisykles, taikomos Taikytinuose teisės aktuose numatytos atsakomybės priemonės.

16. LIABILITY

16.1. Having breached the requirements laid down in General Data Protection Regulation or in other Applicable Laws, or having disregarded these Rules, Employees processing Personal Data or Data Protection Officers shall be liable to sanctions envisaged in Applicable Laws.

17. BAIGIAMOSIOS NUOSTATOS

17.1. Taisyklių laikymosi priežiūra ir, esant poreikiui, peržiūra, patikima Grupės Duomenų apsaugos pareigūnui. Taisyklės yra peržiūrimos (esant poreikiui, atnaujinamos) kasmet, arba tada, kai pasikeičia Taikytini teisės aktai. Taisyklės keičiamos Valdymo įmonės vadovo įsakymu.

17.2. Jeigu kuri nors šių Taisyklių ar kito Grupės ar Grupės įmonės dokumento, reglamentuojančio Asmens duomenų apsaugą, nuostata taps negalima ar prieštaraujančia Taikytiniems teisės aktams, arba dėl kurios nors priežasties taps dalinai arba visai negaliojančia, ji nedarys negaliojančiomis likusių Taisyklių nuostatų.

17. FINAL PROVISIONS

17.1. Compliance monitoring and, if necessary, revision of these Rules shall be carried out by Data Protection Officer. Rules shall be revised (and if necessary, updated) annually or when changes are made to Applicable Laws. Rules shall be amended by the order of Management Company's CEO.

17.2. If any provision of these Rules or of any other Group or Group Company document governing the protection of Personal Data is found to be unenforceable or contrary to Applicable Laws, or becomes fully or partially invalid for whatever reason, the validity of the remaining provisions of these Rules will not be affected.

18. TAISYKLIŲ PRIEDAI

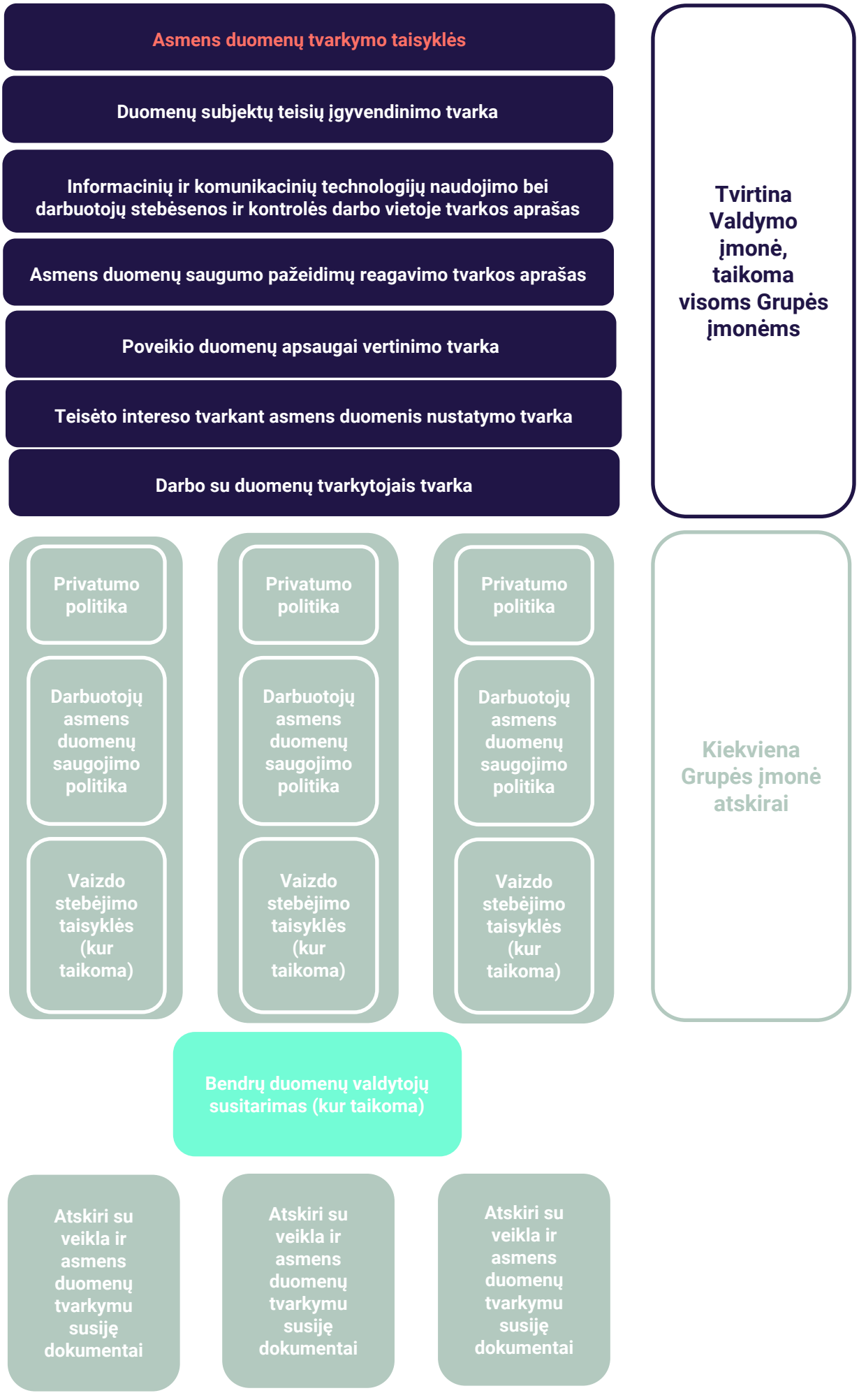
18.1. Šie Taisyklių priedai sudaro neatskiriamą Taisyklių dalį:

18. ANNEXES TO THE RULES

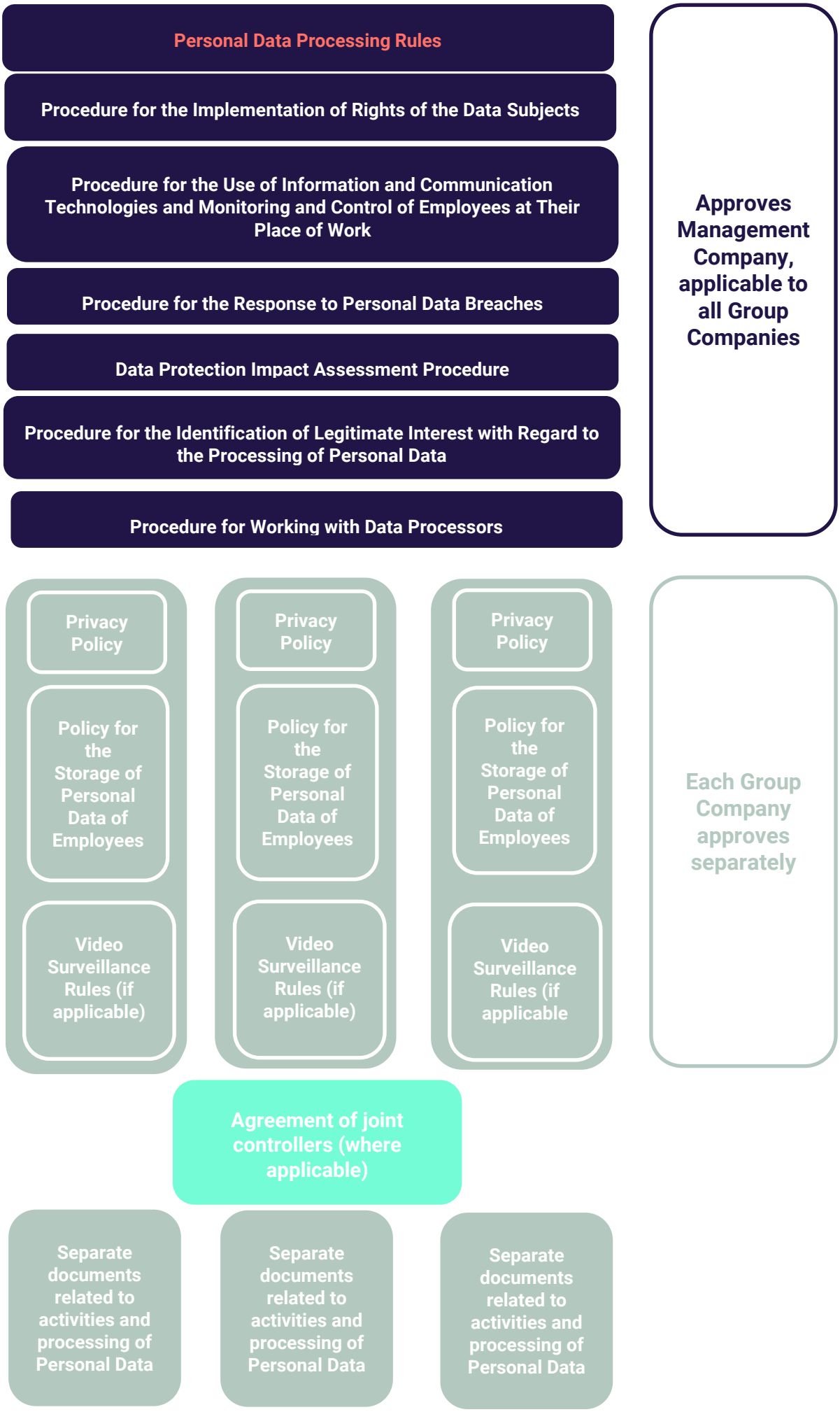
18.1. The following Annexes shall constitute an integral part of these Rules.

1 priedas. Vidinių dokumentų, reglamentuojančių Asmens duomenų apsaugą Grupėje ir Grupės įmonėse, rodyklė;	Annex 1: Index of Internal Documents Governing Personal Data Protection in the Group and Group Companies;
2 priedas. Informacija, kuri pagal BDAR 13 ir 14 straipsnius turi būti pateikta Duomenų subjektui;	Annex 2: Information to be Provided to Data Subjects According to Articles 13 and 14 of GDPR;
3 priedas. Atmintinės darbuotojams dėl tiesioginės rinkodaros, renginių ir nuotraukų bei vaizdo įrašų.	Annex 3: Memos to Employees on Direct Marketing, Events, Images and Videos.

1 priedas


Asmens duomenų tvarkymo taisyklės
Duomenų subjektų teisių įgyvendinimo tvarka
Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje tvarkos aprašas
Asmens duomenų saugumo pažeidimų reagavimo tvarkos aprašas
Poveikio duomenų apsaugai vertinimo tvarka
Teisėto intereso tvarkant asmens duomenis nustatymo tvarka
Darbo su duomenų tvarkytojais tvarka
Tvirtina Valdymo įmonė, taikoma visoms Grupės įmonėms
Privatumo politika
Darbuotojų asmens duomenų saugojimo politika
Vaizdo stebėjimo taisyklės (kur taikoma)
Privatumo politika
Darbuotojų asmens duomenų saugojimo politika
Vaizdo stebėjimo taisyklės (kur taikoma)
Privatumo politika
Darbuotojų asmens duomenų saugojimo politika
Vaizdo stebėjimo taisyklės (kur taikoma)
Kiekviena Grupės įmonė atskirai
Bendrų duomenų valdytojų susitarimas (kur taikoma)
Atskiri su veikla ir asmens duomenų tvarkymu susiję dokumentai
Atskiri su veikla ir asmens duomenų tvarkymu susiję dokumentai
Atskiri su veikla ir asmens duomenų tvarkymu susiję dokumentai

Annex 1


Personal Data Processing Rules
Procedure for the Implementation of Rights of the Data Subjects
Procedure for the Use of Information and Communication Technologies and Monitoring and Control of Employees at Their Place of Work
Procedure for the Response to Personal Data Breaches
Data Protection Impact Assessment Procedure
Procedure for the Identification of Legitimate Interest with Regard to the Processing of Personal Data
Procedure for Working with Data Processors
Approves Management Company, applicable to all Group Companies
Privacy Policy
Policy for the Storage of Personal Data of Employees
Video Surveillance Rules (if applicable)
Privacy Policy
Policy for the Storage of Personal Data of Employees
Video Surveillance Rules (if applicable)
Privacy Policy
Policy for the Storage of Personal Data of Employees
Video Surveillance Rules (if applicable
Each Group Company approves separately
Agreement of joint controllers (where applicable)
Separate documents related to activities and processing of Personal Data
Separate documents related to activities and processing of Personal Data
Separate documents related to activities and processing of Personal Data

2 priedas

INFORMACIJA, KURI PAGAL BDAR 13 IR 14 STRAIPSNIUS TURI BŪTI PATEIKTA DUOMENŲ SUBJEKTUI

Reikalaujamos pateikti informacijos pobūdis	Susijęs straipsnis (jei asmens duomenys renkami tiesiogiai iš duomenų subjekto)	Susijęs straipsnis (jei asmens duomenys gaunami ne iš duomenų subjekto (registrai ir kita)	Pastabos dėl informacijos reikalavimo
Duomenų valdytojo ir, jei taikoma, jo atstovo tapatybė ir kontaktiniai duomenys	13 straipsnio 1 dalies a punktas	14 straipsnio 1 dalies a punktas	Naudojantis šia informacija turi būti galima lengvai nustatyti Duomenų valdytojo tapatybę ir, pageidautina, įvairiu būdu susisiekti su Duomenų valdytoju (pvz., turėtų būti nurodytas telefono numeris, el. pašto adresas, pašto adresas ir t. t.).
Duomenų apsaugos pareigūno, jei taikoma, kontaktiniai duomenys	13 straipsnio 1 dalies b punktas	13 straipsnio 1 dalies b punktas	Nurodomi Grupės ar atskiros Grupės įmonės Duomenų apsaugos pareigūno kontaktai (vardas, pavardė, el. pašto adresas, adresas).
Duomenų tvarkymo tikslai ir teisinis pagrindas	13 straipsnio 1 dalies c punktas	14 straipsnio 1 dalies c punktas	Duomenų tvarkymo tikslą ir pagrindą galima pasitiksinti Duomenų tvarkymo veiklos įrašuose.
Jei duomenų tvarkymo teisinis pagrindas yra teisėti interesai (6 straipsnio 1 dalies f punktas), teisėti interesai, kurių siekia Duomenų valdytojas arba Trečioji šalis	13 straipsnio 1 dalies d punktas	14 straipsnio 2 dalies b punktas	Duomenų subjektui turi būti nurodytas konkretus teisėtas interesas. Pavyzdžiui, teisėtas interesas užtikrinti Grupės Įmonės ir Duomenų subjektų saugumą.
Susijusių asmens duomenų kategorijos	Nereikalaujama	14 straipsnio 1 dalies d punktas	Šią informaciją reikalaujama pateikti 14 straipsnyje nustatyta tvarka, nes Asmens duomenys buvo gauti ne iš Duomenų subjekto, todėl jis/ ji nėra pakankamai informuotas apie tai, kokių kategorijų Asmens duomenis Duomenų valdytojas gavo.
Asmens duomenų gavėjai (arba jų kategorijos)	13 straipsnio 1 dalies e punktas	14 straipsnio 1 dalies e punktas	Gavėjas yra fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuriai atskleidžiami asmens duomenys, nesvarbu, ar tai trečioji šalis ar ne. Gavėjai yra kiti Duomenų valdytojai, bendri duomenų valdytojai ir Duomenų tvarkytojai, kuriems perduodami arba atskleidžiami Asmens duomenys. Pavyzdžiui, Valstybinė mokesčių inspekcija, bankai, notarai, kitos Grupės įmonės ir kt. Galima nurodyti tik duomenų gavėjų kategorijas, pavyzdžiui, paslaugų teikėjai ir kt.
Išsami informacija apie Asmens duomenų perdavimą Trečiosioms valstybėms, tokio perdavimo faktą ir išsami informacija apie	13 straipsnio 1 dalies f punktas	14 straipsnio 1 dalies f punktas	Turėtų būti nurodytas susijęs BDAR straipsnis, pagal kurį leidžiama perduoti duomenis, ir atitinkamas mechanizmas (pvz., sprendimas dėl tinkamumo pagal 45 straipsnį, įmonei privalomos

Reikalaujamos pateikti informacijos pobūdis	Susijęs straipsnis (jei asmens duomenys renkami tiesiogiai iš duomenų subjekto)	Susijęs straipsnis (jei asmens duomenys gaunami ne iš duomenų subjekto (registrai ir kita)	Pastabos dėl informacijos reikalavimo
atitinkamas apsaugos priemones (įskaitant tai, ar Komisija yra priėmusi sprendimą dėl tinkamumo), būdus, kaip gauti jų kopiją, arba apie tai, kur suteikiama galimybė su jais susipažinti.			taisyklės pagal 47 straipsnį, standartinės duomenų apsaugos sąlygos pagal 46 straipsnio 2 dalį ir (arba) nukrypti leidžiančios nuostatos ir apsaugos priemonės pagal 49 straipsnį, ir t. t.). Taip pat turėtų būti pateikta informacija apie tai, kur ir kaip galima susipažinti su atitinkamu dokumentu arba jį gauti, pavyzdžiui, šiuo tikslu pateikiant nuorodą į taikytą mechanizmą. Pagal sąžiningumo principą, apie Asmens duomenų perdavimą Trečiosioms valstybėms teikiama informacija turėtų būti kuo prasmingesnė Duomenų subjektams; paprastai tai reiškia, kad turi būti konkrečiai įvardytos Trečiosios valstybės.
Saugojimo laikotarpis (arba, jei jo nurodyti neįmanoma, kriterijai, pagal kuriuos jis nustatomas)	13 straipsnio 2 dalies a punktas	14 straipsnio 2 dalies a punktas	Asmens duomenų saugojimo laikotarpį galima pasitikslinti Duomenų tvarkymo veiklos įrašuose. Bendras saugojimui terminui taikomas principas: Asmens duomenys neturi būti saugomi ilgiau, negu reikia tikslams dėl kurių jie yra tvarkomi pasiekti.
Duomenų subjektų teisės į: • prieigą prie duomenų; • klaidų ištaisymą; • duomenų ištrynimą; • duomenų tvarkymo apribojimą; • nesutikimą, kad duomenys būtų tvarkomi; • duomenų perkeliamumą.	13 straipsnio 2 dalies b punktas	14 straipsnio 2 dalies c punktas	Šios Duomenų subjektų teisės išsamiai yra paaiškintos Grupės privatumo politikoje. Arba galima nurodyti šią informaciją: • Prieiga prie duomenų: Jei mes saugome ar bet kokiu būdu naudojame Jūsų asmens duomenis, Jūs turite teisę su jais susipažinti. Norėdami tai padaryti, pateikite mums rašytinį prašymą dap@akolagroup.lt. • Klaidų ištaisymas: Jūs turite teisę prašyti mūsų ištaisyti bet kokius turimų duomenų netikslumus. Tokiu atveju mes galime paprašyti Jūsų patvirtinti ištaisytą informaciją. • Duomenų ištrynimas: Jūs turite teisę prašyti mūsų ištrinti Jūsų asmens duomenis. Ši teisė įgyvendinama Bendrojo duomenų apsaugos reglamento 17 straipsnyje numatytais atvejais. • Duomenų tvarkymo apribojimas: Jūs turite teisę prašyti mūsų riboti Jūsų asmens duomenų tvarkymą arba jų netvarkyti. • Nesutikimas, kad duomenys būtų tvarkomi: Jūs turite teisę, Taikomuose teisės aktuose nurodytais atvejais,

Reikalaujamos pateikti informacijos pobūdis	Susijęs straipsnis (jei asmens duomenys renkami tiesiogiai iš duomenų subjekto)	Susijęs straipsnis (jei asmens duomenys gaunami ne iš duomenų subjekto (registrai ir kita)	Pastabos dėl informacijos reikalavimo
			nesutikti, kad mes naudotumėme Jūsų asmens duomenis. • Duomenų perkeliamumas: Jūs turite teisę į duomenų, kuriuos iš Jūsų gavome Jums sutinkant arba sutarties sudarymo tikslais, perkėlimą. Jums pasinaudojus šia teise, Jūsų prašymu perkelsime Jūsų pateiktų duomenų kopiją.
Jei Asmens duomenų tvarkymas grindžiamas sutikimu (arba aiškiu sutikimu), teisė bet kada atšaukti sutikimą	13 straipsnio 2 dalies c punktas	14 straipsnio 2 dalies d punktas	Pateikiant šią informaciją, turėtų būti nurodyta, kaip galima atšaukti sutikimą, užtikrinant, kad atšaukti sutikimą Duomenų subjektui turėtų būti taip pat lengva, kaip ir jį duoti. Pavyzdžiui, nurodyti, kad sutikimą galima atšaukti išsiuntus pranešimą Duomenų apsaugos pareigūnui ar pateikti aktyvią nuorodą.
Teisė pateikti skundą priežiūros institucijai	13 straipsnio 2 dalies d punktas	14 straipsnio 2 dalies e punktas	Jeigu manote, kad jūsų asmens duomenis tvarkome netinkamai, galite pateikti skundą priežiūros institucijai: • Lietuvoje Valstybinei duomenų apsaugos inspekcijai (www.vdai.lrv.lt); • Latvijoje: Datu Valsts inspekcija, (https://www.dvi.gov.lv/); • Estijoje: Andmekaitse inspektsioon, (https://www.aki.ee/).
Tai, ar informacijos pateikimas yra teisės aktais arba sutartyje numatytas reikalavimas, ar reikalavimas, kurį būtina įvykdyti norint sudaryti sutartį, arba ar yra nustatyta prievolė pateikti šią informaciją, ir informacija apie galimas tokių duomenų nepateikimo pasekmes.	13 straipsnio 2 dalies e punktas	Nereikalaujama	Internetinėse formose turėtų būti aiškiai nurodyta, kuriuos laukus privaloma užpildyti, kurių užpildyti nebūtina ir kokios bus privalomų laukų neužpildymo pasekmės.
Asmens duomenų kilmės šaltinis, ir, jei taikoma, ar tie duomenys gauti iš viešai prieinamo šaltinio	Nereikalaujama	14 straipsnio 2 dalies f punktas	Turėtų būti nurodytas konkretus Asmens duomenų šaltinis, išskyrus atvejus, kai to padaryti neįmanoma. Jei konkretus šaltinis neįvardijamas, pateikiant informaciją reikėtų nurodyti: šaltinių pobūdį (t. y. ar šaltiniai priklauso viešiesiems, ar privatiems subjektams) ir organizacijų, pramonės šakų ir (arba) sektorių

Reikalaujamos pateikti informacijos pobūdis	Susijęs straipsnis (jei asmens duomenys renkami tiesiogiai iš duomenų subjekto)	Susijęs straipsnis (jei asmens duomenys gaunami ne iš duomenų subjekto (registrai ir kita)	Pastabos dėl informacijos reikalavimo
			tipus. Pavyzdžiui, Asmens duomenys gauti iš VĮ „Registrų centras“.
Tai, kad esama automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, jei taikoma, prasminga informacija apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui	13 straipsnio 2 dalies f punktas	14 straipsnio 2 dalies g punktas	Jeigu sprendimą, kuris turės svarbių pasekmių Duomenų subjektui (nebus skiriamas kreditas, suteikta darbo vieta ir kt.), priima algoritmas, tuomet Duomenų subjektas turi būti apie tai informuotas. Be to, Duomenų subjektui turi būti suteikta galimybė pateikti prašymą, kad algoritmo priimtą sprendimą peržiūrėtų žmogus.

Annex 2

INFORMATION TO BE PROVIDED TO DATA SUBJECTS ACCORDING TO ARTICLES 13 AND 14 OF GDPR

Required Information Type	Relevant article (if Personal Data collected directly from Data Subject)	Relevant article (if Personal Data not obtained from the Data Subject)	Comments on information requirement
The identity and contact details of the Controller and, where applicable, their representative	Article 13.1 (a)	Article 14.1 (a)	This information should allow for easy identification of the Controller (usually Group or Group Company) and preferably allow for different forms of communications with the Personal Data Controller (e.g. phone number, email, postal address, etc.)
Contact details for the Data Protection Officer, where applicable	Article 13.1 (b)	Article 14.1 (b)	Contact details of Group or Group Company Data Protection Officer (name, surname, email, address).
The purposes and legal basis for the processing	Article 13.1 (c)	Article 14.1 (c)	The purpose and legal basis of Data Processing can be checked at the Records of Data Processing.
Where legitimate interests (Article 6.1(f)) is the legal basis for the Personal Data Processing, the legitimate interests pursued by the Personal Data Controller or a Third Party	Article 13.1 (d)	Article 14.2 (b)	The specific interest in question must be identified for the benefit of the Data Subject. For example, legitimate interest to ensure Group Company and Data subjects safety.
Categories of Personal Data concerned	Not required	Article 14.1 (d)	This information is required in an Article 14 scenario because the Personal Data has not been obtained from the Data Subject, who therefore lacks an awareness of which categories of their Personal Data the Controller has obtained.
Recipients (or categories of recipients) of the Personal Data	Article 13.1 (e)	Article 14.1 (e)	Recipient is a natural or legal person, public authority, agency, or another body, to which the Personal Data are disclosed, whether a Third Party or not. Therefore, other Controllers, joint controllers and Processors to whom Personal Data is transferred or disclosed are covered by the term recipient. For example, State Tax Authority, bank, notary, other Group Companies, etc. As well only categories of recipients can be stated, e. g., service providers, etc.
Details of transfers to Third Countries, the fact of same and the details of the	Article 13.1 (f)	Article 14.1 (f)	The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article

Required Information Type	Relevant article (if Personal Data collected directly from Data Subject)	Relevant article (if Personal Data not obtained from the Data Subject)	Comments on information requirement
relevant safeguards (including the existence or absence of a Commission adequacy decision) and the means to obtain a copy of them or where they have been made available			45; binding corporate rules under Article 47; standard data protection clauses under Article 46.2; derogations and safeguards under Article 49, etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e. g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to Third Countries should be as meaningful as possible to Data Subjects; this will generally mean that the Third Countries be named.
The storage period (or if not possible, criteria used to determine that period)	Article 13.2 (a)	Article 14.2 (a)	Personal Data storage period can be checked at Records of Processing Activities. The general principle of the storage period is that Personal Data must not be kept longer than necessary for the purposes for which it is processed.
The rights of the data subject to: • access; • rectification; • erasure; • restriction on processing; • objection to processing; and • portability.	Article 13.2 (b)	Article 14.2 (c)	The following Data Subjects' rights are explained in the Group Privacy policy. However, the following information can be presented: • **Right to access**: You can contact us at any time and ask if we process any of your personal data. If we store or use your personal data in any way, you have the right to access them. If you wish to do this, please submit a written request to us by dap@akolagroup.lt. • **Right to rectification**: You have the right to request us to rectify any inaccuracies of data held by us. In this case, we may ask you to confirm the rectified information. • **Right to erasure**: You have the right to ask us to erase your personal data. This right will be implemented in cases provided in Article 17 of the General Data Protection Regulation • **Right to restrict processing**: You have the right to ask us to restrict the processing of your personal data or to object to their processing. • **Right to object processing**: You have the right to object processing of your personal data by us.

Required Information Type	Relevant article (if Personal Data collected directly from Data Subject)	Relevant article (if Personal Data not obtained from the Data Subject)	Comments on information requirement
			• **Right to portability**: You have the right to the portability of data obtained by us under your consent or for the purpose of agreement conclusion. If you exercise this right, we will transfer a copy of the data provided by you.
Where processing is based on consent (or explicit consent), the right to withdraw consent at any time	Article 13.2 (c)	Article 14.2 (d)	This information should include how consent may be withdrawn, considering that it should be as easy for a Data Subject to withdraw consent as to give it. For example, inform that consent can be canceled by sending email to Data Protection Officer or provide active hyperlink.
The right to lodge a complaint with a supervisory authority	Article 13.2 (d)	Article 14.2 (e)	If you think that we are processing your personal data incorrectly, you can file a complaint with the supervisory authority: Lithuania: Valstybinė duomenų apsaugos inspekcija (www.vdai.lrv.lt). Latvia: Datu Valsts inspekcija, (https://www.dvi.gov.lv/) Estonia: Andmekaitse inspektsioon, (https://www.aki.ee/).
Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.	Article 13.2 (e)	Not required	The online forms should clearly indicate which fields are “required”, which are optional and what the consequences of not filling in the required fields will be.
The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source	Not required	Article 14.2 (f)	The specific source of the data should be provided unless it is not possible to do so. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly or privately held sources) and the types of organization/ industry/ sector. For example, Personal Data is received from “State Registry”.
The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and	Article 13.2 (f)	Article 14.2 (g)	If a decision that will have important consequences for the Data Subject (e. g., decision to refuse granting a credit) is made by the algorithm, then the Data Subject must be informed. In addition, the

Required Information Type	Relevant article (if Personal Data collected directly from Data Subject)	Relevant article (if Personal Data not obtained from the Data Subject)	Comments on information requirement
envisaged consequences of such processing for the Data Subject			Data Subject must be given the opportunity to request that the decision made by the algorithm be reviewed by a human.

3 priedas

ATMINTINĖ DARBUOTOJAMS DĖL TIESIOGINĖS RINKODAROS, RENGINIŲ IR NUOTRAUKŲ BEI VAIZDO ĮRAŠŲ

1. KAM SKIRTA ŠI ATMINTINĖ

Ši atmintinė (toliau – **Atmintinė**) skirta visiems [pavadinimas] (toliau – **Bendrovė)** darbuotojams, tiesiogiai bendraujantiems su klientais ir teikiantiems jiems pasiūlymus, organizuojantiems renginius ir šventes klientams, darbuotojams ar jų vaikams, taip pat naudojantiems asmenų nuotraukas / filmuotą medžiagą, tvarkantiems socialinių tinklų paskyras: pardavimo vadybininkams, administratoriams, marketingo specialistams, personalo skyriaus darbuotojams ir kt. Atmintinė padės tiesioginės rinkodaros, pardavimų ir renginių vykdymo metu išvengti Bendrojo duomenų apsaugos reglamento (toliau – **BDAR**) pažeidimų.

2. TIESIOGINĖ RINKODARA

2.1. Kas yra tiesioginė rinkodara?

Tiesioginė rinkodara - tai pasiūlymų siuntimai faksu, paštu, el. paštu, SMS žinutėmis, siūlymai telefonu. Apklausa dėl vartotojų nuomonės tyrimo ar užklausos dėl prekių ar paslaugų kokybės taip pat yra tiesioginė rinkodara. Tokie pranešimai toliau vadinami **Pasiūlymu**.

Atmintinė taikoma tada, kai Pasiūlymai siunčiami **fiziniams asmenims arba įmonių darbuotojams, kuriuos galima identifikuoti** (pvz. vardas.pavarde@imone.lt). Bendri įmonės kontaktai (pvz. info@... office@...) nelaikomi asmens duomenimis, tačiau siunčiant Pasiūlymus įmonės kontaktais, taip pat reikia vadovautis toliau pateikiamomis taisyklėmis. Juridinio asmens sutikimas yra laikomas tinkamu, jei yra duotas tokio juridinio asmens darbuotojo, kuris turi teisę veikti įmonės vardu.

2.2. Tiesioginę rinkodarą vykdyti galima tik vienu iš šių atvejų:

(i) Asmuo yra davęs sutikimą gauti tiesioginės rinkodaros pasiūlymus; arba

(ii) Asmuo yra klientas, t. y., asmuo įsigijo prekių (sėklų, trąšų) ar paslaugų (remonto darbai, elevatoriaus nuoma) ne vėliau nei prieš 2 (dvejus) metus. Jeigu asmeniui siūloma žemės ūkio technika, tuomet asmuo turi būti įsigijęs žemės ūkio technikos ne vėliau nei prieš 5 (penkerius) metus. Šiuo atveju be asmens sutikimo tiesioginė rinkodara galima **tik el. paštu** ir tik dėl **savo pačių prekių ar paslaugų** (pvz., AB „Linas Agro“ gali siūlyti savo klientams savo prekes ar paslaugas, bet negali siūlyti žemės ūkio technikos, kuria prekiauja UAB „Dotnuva Baltic“).

Lentelėje pateikiamos sąlygos, atitikimą kurioms reikia patikrinti prieš asmenims siunčiant pasiūlymus:

YRA GAUTAS SUTIKIMAS	ASMUO YRA ESAMAS KLIENTAS	PASIŪLYMAI SIUNČIAMI BENDRUOJU ĮMONĖS EL. PAŠTU
Sąlygos: 1. Patikrinus, ar yra duotas asmens sutikimas (žr. žemiau); 2. Patikrinus, ar sutikimas yra duotas konkretiems veiksmams (pasiūlymams, nuomonės tyrimui, kt.); 3. Patikrinus, ar asmuo neišreiškė noro gauti informaciją konkrečia ryšio priemone (pvz., skambinti telefonu, siųsti SMS); 4. Patikrinus, ar po sutikimo gavimo nepraėjo 3 metai; 5. Asmuo turi būti aiškiai sutikęs gauti kitų grupės įmonių ar partnerių	Sąlygos: 1. Pasiūlymas tik el. paštu; 2. Tik esamiems klientams; 3. Panaši tik pačios Bendrovės (ne kitų grupės įmonių ar partnerių) prekė ar paslauga, kurią anksčiau klientas įsigijo ir (ar) užsisakė; 4. Klientas anksčiau neprieštaravo dėl Pasiūlymų gavimo (sistemoje nėra įrašų ir klientas žodžiu nepareiškė prieštaravimų, sutikimo formoje nepažymėta, nei „sutinku“, nei „nesutinku“); 5. Asmeniui kiekviename pranešime nurodoma, kad	Sąlygos: 1. Pasiūlymai siunčiami tik el. paštu. 2. Tik bendruoju Bendrovės el. paštu. 3. Bendrovė anksčiau nėra prieštaravusi Pasiūlymų gavėjui. 4. Bendrovė kiekviename pranešime informuojama, kad ji turi galimybę prieštarauti dėl Pasiūlymų pateikimo.

(trečiosios šalys) pasiūlymus (jeigu taikoma); 6. Suteikiama informacija apie tai, kaip atsisakyti pasiūlymo; 7. Daroma nuoroda į privatumo politiką.	jis turi galimybę atsisakyti Pasiūlymų siuntimo; 6. Klientas įsigijo prekę (sėklas, trąšas) ar paslaugą (remonto darbus) ne anksčiau nei prieš 2 metus. Jeigu siūloma žemės ūkio technika, tuomet ne anksčiau nei prieš 5 metus; 7. Daroma nuoroda į privatumo politiką.	

2.3. Kaip gali būti gaunamas sutikimas Pasiūlymams?

- **Elektroniniu būdu** (renkama per Bendrovės interneto svetainę, socialinius tinklus ir pan.). Prieš pradedant naują kampaniją, rekomenduotina suderinti ją su teisės skyriumi.

- **Susitikus su asmeniu** (asmeniniame susitikime, renginyje ar kt.), **paprašyti pasirašyti nustatytą sutikimo formą gauti Pasiūlymus**. Reikia informuoti asmenį, kad jam atsisakius pasirašyti sutikimo formą galimybės jam atsiųsti Pasiūlymą nebus.

- **Jei asmuo pats paskambina telefonu**, norėdamas gauti Pasiūlymą, turi būti paprašoma, kad klientas parašytų trumpą užklausimą vadybininko el. paštu ar mobiliuoju telefonu. Pasiūlymą rekomenduojama siųsti tik tada, kai toks užklausimas yra gautas (užklausimą reikia pažymėti sistemoje).

- Asmuo gali išreikšti savo sutikimą ir **atsiųsdamas elektroninį laišką**, kuriame aiškiai duotas sutikimas ar prašymas/užklausimas atsiųsti Pasiūlymą. Tokiu atveju galima tik atsakyti į užklausą, o pasibaigus bendravimui, jei nėra bendro sutikimo dėl Pasiūlymų siuntimo, arba jei jis netapo klientu (kaip nustatyta 3 punkte), tolesnių Pasiūlymų siųsti negalima.

2.4. Kaip išsaugoti sutikimą?

Darbuotojai turi pareigą surinkti ir saugoti asmenų duotus sutikimus. Visi darbuotojo rašytine forma gauti asmenų sutikimai ne vėliau nei kitą darbo dieną turi būti nuskenuoti ir išsaugoti Bendrovės serveryje tam skirtame kataloge / Scoro sistemoje.

2.5. Pasiūlymų siuntimas

Pirmo kreipimosi ryšio priemonėmis metu, kai asmuo yra davęs sutikimą šioje Atmintinėje nustatyta tvarka, Pasiūlymo gavėjui privaloma pateikti nuorodą į Privatumo politiką. Taip pat rekomenduotina darbuotojo paraše padaryti nuorodą į Privatumo politiką.

Rekomenduojama pirmą pasiūlymą išsiųsti ne vėliau kaip per pusę metų nuo sutikimo gavimo datos.

Kiekvieną kartą siunčiant Pasiūlymą ryšio priemonėmis, **būtina informuoti klientą, kad jis turi galimybę atsisakyti pasiūlymų siuntimo ir nurodyti atsisakymo tvarką.**

2.6. Sutikimų atšaukimas, atsisakymas ir prieštaravimas

Jei asmuo nesutiko/atsisakė Pasiūlymų gavimo, nutraukė naujienlaiškių prenumeravimą ar pareiškė skundą dėl Pasiūlymų siuntimo ir siūlymo, darbuotojas turi pareigą nedelsiant užfiksuoti gautą atsisakymą/prašymą/skundą duomenų bazėje prie kliento duomenų ir imtis kitų veiksmų pagal atitinkamas Bendrovės tvarkas.

2.7. Bet kokiomis aplinkybėmis draudžiama:

- Pirkti ir naudotis duomenų bazėmis, kontaktus rinkti internete.

- Gautus asmens duomenis perduoti ar atskleisti įmonėms, kurios nėra AB Akola group dalis (dalintis asmens duomenimis Grupės viduje galima tik, jei gautas sutikimas tai leidžia), ar privatiems asmenims, jei klientas dėl to aiškiai nesutiko.

- Siųsti Pasiūlymų elektroniniu paštu, SMS žinutėmis, faksu ar kitomis priemonėmis, *siekiant gauti sutikimą tolimesniems pasiūlymų siuntimams* (pvz., „ar sutinkate gauti pasiūlymus ateityje?“), be asmens sutikimo, kadangi **tai jau yra tiesioginė rinkodara** ir jai reikia gauti sutikimą.

3. RENGINIAI IR ŠVENTĖS

3.1. Filmavimas / fotografavimas

Asmenys (Klientai, darbuotojai, darbuotojų vaikai, renginių dalyviai ir kt.) turi teisę nuspręsti, kur ir kada galima juos fotografuoti / filmuoti ir skelbti jų nuotraukas, todėl **reikia gauti asmenų sutikimus juos filmuoti/ fotografuoti ir skelbti jų nuotraukas.**

Svarbu, jog **asmens sutikimas būti filmuojamu /fotografuojamu nėra asmens sutikimas nuotraukas publikuoti**. Jeigu asmenų (darbuotojų, klientų) nuotraukomis norima pasidalinti socialiniuose tinkluose, interneto tinklapyje ar intranete (naujienlaiškyje ir pan.) **reikia gauti jų sutikimus**.

Vaikų (asmenų iki 18 metų) fotografavimui/filmavimui bei nuotraukų publikavimui reikia gauti tėvų ar globėjų sutikimus. Jeigu renginys skirtas darbuotojų vaikams ir jame bus filmuojama / fotografuojama, prieš renginį **reikia gauti darbuotojų sutikimus dėl jų vaikų nuotraukų ar vaizdo įrašų darymo ir publikavimo**.

Sutikimas turi būti išreikštas rašytine, elektronine ar kita forma (svarbu, kad Bendrovė vėliau galėtų įrodyti, kad sutikimą turėjo). Jeigu prašoma kliento leisti pasidalinti jo nuotrauka socialiniuose tinkluose ar interneto svetainėje, prie prašymo visada turi būti pateikta nuoroda į Privatumo politiką.

3.2. Kvietimai į renginius / informavimas

Jeigu renginių metu ketinama filmuoti ar fotografuoti asmenis, kvietimuose į renginius nurodoma, jog: „*Renginio metu galite būti filmuojami / fotografuojami, o nuotraukos / filmuota medžiaga naudojama [nurodyti, kokios Bendrovės ir/ar partnerių, kitų renginio organizatorių] [nurodyti, kokiu tikslu naudojama: renginio viešinimo tikslu, reklamai ir pan.]. Jeigu nesutinkate būti filmuojami / fotografuojami, renginio dieną praneškite apie tai organizatoriams [nurodyti, kokiu būdu: el.paštu, dalyvių registratoriams ar pan.], ir organizatoriai Jums nurodys zonas, kuriose nėra fotografuojama / filmuojama*.“ Renginio vietoje paskirkite zoną, kurioje esantys asmenys nebus fotografuojami / filmuojami.

Jeigu dėl renginio dydžio (pvz., didelė žemės ūkio paroda) nėra galimybių užtikrinti zonų, kuriose dalyviai nebūtų filmuojami ar fotografuojami, galima nurodyti tokį pranešimą: „*Renginio metu galite būti filmuojami / fotografuojami, o nuotraukos / filmuota medžiaga naudojama [nurodyti, kokios Bendrovės ir/ar partnerių, kitų renginio organizatorių] [nurodyti, kokiu tikslu naudojama: renginio viešinimo tikslu, reklamai ir pan.]. Atsižvelgiant į renginio masiškumą, organizatoriai negali užtikrinti kiekvieno renginio dalyvio teisės nebūti filmuojamiems ar fotografuojamiems renginio metu. Mes pasižadame tokios medžiagos naudojimu nepažeisti Jūsų garbės ir orumo. Jeigu norite, kad paskelbta Jūsų nuotrauka iš renginio būtų pašalinta, praneškite apie el. paštu: [el.paštas]*.“

4. NUOTRAUKOS / VAIZDO ĮRAŠAI

4.1. Nuotraukų / vaizdo įrašų darymas

Informuokite fotografus / operatorius, jog jeigu asmuo slepiasi (užsidengia veidą), nepozuoja ar aiškiai pasako, kad nenori būti fotografuojamas / filmuojamas, tokių asmenų negalima fotografuoti / filmuoti.

Jeigu renginio metu bus fiksuojamas panoraminis vaizdas, kuriame neišryškinami konkretūs žmonės, sutikimai nereikalingi.

4.2. Nuotraukų / vaizdo įrašų naudojimas

Asmenys turi teisę nuspręsti, kur ir kada galima skelbti jų atvaizdus.

Prieš skelbdami asmenų (darbuotojų, klientų ar kt.) nuotraukas / video turinį iš renginių ar švenčių (net jeigu gautas asmens sutikimas), turi būti įvertinta ar nuotraukos / filmuota medžiaga nežeis juose vaizduojamų asmenų.

Jeigu asmuo paprašytų pašalinti paskelbtas jo nuotraukas ar video turinį, tai turi būti padaryta. Skelbiamame albume gali būti nurodyta: „*Jeigu norite, kad paskelbta Jūsų nuotrauka/video būtų pašalinta, praneškite el. paštu: [el.paštas]*.“

Svarbu, jog asmeniui atšaukus duotą sutikimą, neturi būti pašalintos nuotraukos ar kita informacija, kuri buvo surinkta sutikimo pagrindu. Sutikimo atšaukimas turės pasekmes tik tolimesniam duomenų tvarkymui, t. y. duomenys nebegalės būti tvarkomi, pvz. tokio asmens nuotraukų nebegalima skelbti, remiantis jo sutikimu.

4.3. Nuotraukų / vaizdo įrašų saugojimas

BDAR neleidžia saugoti asmens duomenų neribotą laiką ir reikalauja nusistatyti laiko tarpą, kada asmens duomenys turi būti pašalinti arba kas kiek laiko asmens duomenys turėtų būti peržiūrimi ir įvertinus jų aktualumą pašalinami.

Darbuotojui išėjus iš darbo, jo portretinės nuotraukos (naudojamos kontaktų sąraše ir kt.) turi būti ištrintos iš Bendrovės serverių per vieną mėnesį.

Nuotraukas iš renginių, kurios yra paskelbtos socialiniuose tinkluose ar Bendrovės interneto svetainėse, rekomenduojame peržiūrėti kasmet (pvz., sausio mėnesį) ir pašalinti nebeaktualias nuotraukas ar įrašus, tačiau nepublikuoti jų socialiniuose tinkluose ar interneto svetainėse **ilgiau nei 5 (penkerius) metus nuo paskelbimo**.

Asmenų nuotraukas iš renginių galima saugoti Bendrovės serveriuose / spintose, tačiau tokias nuotraukas 5 (penkeri) metai po renginio reikėtų peržiūrėti ir pašalinti nebeaktualias (pvz., asmuo jau nebedirba). Be to, prie nuotraukų albumų, kai nuo renginio praėjo daugiau nei 5 (penkeri) metai, turėtų būti apribota prieiga, t. y., ne visi darbuotojai galėtų matyti nuotraukas.

Nuotraukos, kuriose vaizduojami Bendrovei istoriškai svarbūs momentai, gali būti saugomos (archyvuojamos) ilgiau nei 5 (penkerius) metus, tačiau prieiga prie jų privalo būti ribojama.

5. ATSAKOMYBĖ

Už sutikimo gavimą ir išsaugojimą yra atsakingi darbuotojai, tiesiogiai bendraujantys su (potencialiais) klientais, organizuojantys renginį/šventę ar naudojantis (pvz., skelbiantys) nuotraukas ar filmuotą medžiagą.

Darbuotojo veiksmai, pažeidę šioje Atmintinėje nustatytus reikalavimus, gali būti laikomi šiurkščiu darbo pareigų pažeidimu. Taip pat darbuotojas rizikuoja asmeniškai atsakyti už padarytą žalą.

Annex 3

MEMO TO EMPLOYEES ON DIRECT MARKETING, EVENTS, IMAGES AND VIDEOS

1. WHO ARE THE TARGET RECIPIENTS OF THIS MEMO

This memo (the **Memo**) is intended for [name of the company] (**Company**) employees directly communicating with customers and providing them offers, organizing events and celebrations for customers, employees or their children, as well as employees using photos/ videos of individuals, managing social media accounts, i.e. sales managers, administrators, marketers, HR staff, etc. The Memo will help to avoid the breaches of the General Data Protection Regulation (the **GDPR**) in the course of direct marketing and events activities.

2. DIRECT MARKETING

2.1. What is the direct marketing?

Direct Marketing means the submission of offers by fax, post, e-mail, text messages, and phone. Consumer surveys or enquiries regarding the quality of goods or services shall also be considered direct marketing. Such notifications shall hereinafter be referred to as the '**Offer**'.

The Memo shall be used when Offers are sent to natural persons or company employees which can be identified (e.g., name.surname@info.ee). General contact details of a company (e.g., info@..., office@...) shall not be considered personal data (if they do not contain personal data);

2.2. Direct marketing may be carried out only in one of the following cases:

(i) A person (legal person employee or individual) has given his/ her consent to receive direct marketing Offers.

(ii) Email address (legal person employee or individual) was obtained within the framework of the company commercial transactions (A person bought some goods or orders service of the Company). In this case Offers may be sent only by email and only for the Company goods or services. However, the person (legal person employee or individual) must be allowed to opt out at the collection of his / her personal data. E.g., a notice can be added to a contract that: „The company might use your contact details for sending you offers of similar goods or services. Would you like to refuse receiving these offers?

(iii) Offers are sent to general email of the company, e.g. office@company.ee, info@company.ee, etc.

The table sets out the conditions that must be checked before submitting Offers:

CUSTOMER'S CONSENT HAS BEEN OBTAINED	EMAIL WAS OBTAINED IN THE COURSE OF ACTIVITY	OFFERS ARE SENT TO GENERAL EMAIL OF THE COMPANY
Conditions: 1. Having verified if the customer has given their consent (see below); 2. Having verified if the consent has been given for specific actions (offers, surveys, etc.); 3. Having verified if the customer has not expressed their wish to receive information via the specific mean of communication (e.g., by phone, text message); 4. Having verified if 3 year has not passed after the receipt of customer's consent; 5. Explicit consent of the customer to receive partners' (third-party) Offers must be given; 6. Information about the procedure of objection to the Offer shall be provided; 7. Reference to the privacy policy shall be provided.	Conditions: 1. Offers only via e-mail; 2. Only to the customers (person who bought some product or ordered service); 3. Goods or service of the Company itself (not its partners); 4. The customer previously has not objected against the receipt of Offers (there are no records in the system and the customer has not objected verbally, neither 'I consent' nor 'I do not consent' is checked in the form); 5. The person/ customer is informed in every notification that they have the possibility to object against the submission of Offers; 6. Reference to the privacy policy shall be provided.	Conditions: 1. Offers only via email. 2. Only to the general email of the Company. 3. The company previously has not objected against the recipient of the Offers. 4. The company is informed in every notification that they have the possibility to object against the submission of Offers.

2.3. How the customer's consent to the submission of offers may be obtained?

- **Electronically** (collected through the Company's website, social networks, etc.). Before starting a new campaign, it is advisable to reconcile it with the [Legal Department].
- **During the meeting with a person** (in a personal meeting, event, etc.), ask to sign the prescribed consent form to receive the Proposals. The person must be informed that if he refuses to sign the consent form, it will not be possible to send him the Offer.
- **If the customer calls on the phone** and expresses the wish to receive the Offer, they must be requested to send a brief enquiry to the manager's e-mail or mobile phone. The Offer may be submitted only in the case where such enquiry has been received (the enquiry must be saved in the system with the customers data).
- The customer may also express their consent **by sending an e-mail** with the clearly expressed consent or request/enquiry to send the Offer. In this case, it is only permitted to reply to the enquiry, and having completed the communication, if the general consent to the submission of Offers has not been provided or if the person has not become a customer (as provided in Clause 2.2), submission of further Offers is not permitted.

2.4. How to store the consent?

Employees have the obligation to collect and store the consents provided by persons. All consents of persons obtained by the employee in writing shall be scanned on the next working day at the latest and saved on the Company server in the respective catalogue.

2.5. Offer content

Offer must be clearly recognisable as a commercial communication. Also, Offer content must meet the following conditions:

(i) Offer content (for goods or service) and the conditions regarding the receiving of the service or goods must be precisely formulated;

(ii) Discounts, bonuses and prizes must be clearly recognizable;

(iii) Competitions, lotteries or games must be clearly definable and the relevant terms of participation must be easily accessible, as well as clearly outlined;

The person/ company on behalf of whom Offer is distributed must be clearly identifiable.

2.6. Sending the Offers

At the time of first contact with the customer using the communication means, in cases where the customer has provided their consent pursuant to the procedure provided in this Memo, the customer must be provided a link to/information on the Privacy Policy. Also, it is strongly recommended to provide the link to the Privacy Policy in the employee's e-mail signature.

It is recommended that the first Offer be sent no later than six months after the date of receipt of the consent.

Each time when submitting an Offer using communication means, it **is mandatory to inform the customer that they can object against the submission of offers and explain the procedure.**

2.7. Withdrawal of consents of the customers, their refusal and objection

If a person has not consented/refused to receive the Offers, has terminated their newsletter subscription or filed a complaint regarding the submission of notifications and offers, the employee is obligated to promptly record the received refusal/request/complaint in the database along the customer's data and take other actions pursuant to the respective procedures of the Company.

2.8. It shall be forbidden in any circumstances:

- to purchase and use databases, collect the contact details on the internet;
- to transfer or disclose obtained personal data to other companies, which are not part of AB "Akola Group" (sharing of personal data within the group is only permitted if consent is obtained) or private persons if the customer has not given their explicit consent to this;
- to send Offers by e-mail, text messages, fax or using other means in order to obtain person's consent for further submission of Offers without the person's consent, because this in itself is considered the direct marketing activities for which the consent must be obtained. E.g., the following text: 'Do you consent to receive offers in the future?'.

3. EVENTS AND CELEBRATIONS

3.1. Filming / photography

Persons (Clients, employees, employees' children, participants in events, etc.) have the right to decide where and when they can be photographed / filmed and their photos published, therefore the **consent of persons to film / photograph them and publish their photos should be obtained.**

It is important that a **person's consent to be filmed / photographed is not a person's consent to publish photos**. If photos of persons (employees, customers) are to be shared on social networks, on a website or intranet (newsletter, etc.), **their consent must be obtained**.

Photographs / videos of children (persons under 18) and the publication of photographs require the consent of parents or guardians. If the event is for the children of employees and will be filmed / photographed**, the consent of the employees regarding the taking and publication of photos or videos of their children must be obtained before the event.**

If consent is collected it must be expressed in written, electronic or other form (it is important that the company can later prove that it had consent). If a customer is asked to allow their photo to be shared on social networks or on a website, the request must always be accompanied by a link to the Privacy Policy.

3.2. Invitations to events / information

If it is intended to film or photograph event, when individuals must be informed in the invitations to the events that: "*You may be filmed / photographed during the event and the photos / footage will be used by[specify which Company and / or partners, other event organizers] [specify for what purpose used: for the purpose of publicizing the event, for advertising, etc.]. If you do not agree to be filmed / photographed, please notify the organizers on the day of the event [indicate how: by e-mail, to the registrars of the participants, etc.] and the organizers will indicate to you the areas where filming / photographic will not take place.* " individuals must not be photographed / filmed.

If, due to the size of the event (e.g., a large agricultural exhibition), it is not possible to secure areas where participants will not be filmed or photographed, the following message may be indicated: "*You may be filmed / photographed in the event and photographs / footage will be used by the company and / or partners, other event organizers] [specify the purpose for which: the event is used to publicize, advertise, etc.]. Due to the mass of the event, the organizers cannot guarantee the right of each participant of the event not to be filmed or photographed during the event. We promise not to harm your honour or dignity by using such material. If you would like your published photo to be removed from the event, please send us e-mail: [e-mail address]".*

4. PHOTOGRAPHS / VIDEOS

4.1. Taking of photos / videos

Inform photographers / operators that if a person hides (covers their face), does not pose or clearly states that they do not want to be photographed / filmed, such persons may not be photographed / filmed.

If a panoramic image is captured during the event that does not highlight specific people, consents are not required.

4.2. Use of photos/ videos

Individuals have the right to decide where and when their images can be published.

Before publishing photos / videos of individuals (employees, customers, etc.) from events or celebrations (even if consent has been obtained), it must be assessed whether the photos / footage will not offend the individuals depicted in them.

If a person requests the removal of their published photos or video content, this must be done. The album you are posting may say, "If you want your photo / video posted to be removed, please email us by e-mail: [e-mail]. "

It is important that when a person withdraws their consent, no photos or other information that has been collected on the basis of the consent should be removed. Withdrawal of consent will only have consequences for further processing of the data, i.e. data can no longer be processed, e.g. photos of such a person may no longer be published with his or her consent.

4.3. Photo / video storage

The GDPR does not allow the storage of personal data for indefinitely time period and requires to set storage time period for the removal of personal data or the term for review of data collected and removal of it, if it is not required for the purpose for which it was collected.

When an employee terminates his work agreement, his or her portrait photos (used in the contact list, etc.) must be deleted from the Company's servers within one month.

We recommend reviewing photos from events that are posted on social networks or the Company's websites annually (e.g. in January) and remove obsolete photos or records, but do not publish them on social networks or websites for more than **5 (five) years after publication**.

Photos of individuals from the events can be stored on the Company's servers / cabinets, but such photos should be reviewed and removed as obsolete 5 (five) years after the event (e.g., the person is no longer working). In addition, access to photo albums 5 (five) years after the event should be restricted, e. i., not all employees would be able to see the photos.

Photographs depicting moments of historical importance to the Company may be stored (archived) for more than 5 (five) years, but access to them must be restricted.

5. LIABILITY

Employees communicating with the customers directly, organizing events / celebrations, or using (e. g., posting) photos or videos materials shall be responsible for the receipt and storage of consents.

Employee's actions in violation to the requirements established in this Memo may be considered a severe violation of work duties. Also, the employee may be obligated to assume personal liability for the incurred damage.