Does locating pets qualify as processing of personal data?

Pauliina Vilponen, 503708

OTMU2247 Property Law

University of Turku

Faculty of Law

June 2018

Abstract

UNIVERSITY OF TURKU
Faculty of Law
VILPONEN, PAULIINA: Does locating pets qualify as processing of personal data?
Pro gradu -thesis, 80 p.
OTMU2247 Property Law
June 2018

One noteworthy and unconventional form of data processing is accessing location information on an electronic collar worn by a pet. Technically, this kind of data collection is conducted within a mobile application operated on a mobile device. The collected location data closely connects to the location of the pet owner or another individual residing close to the pet. Therefore, the app developer operating the mobile application must comply with all relevant data protection legislation.

The first part of this thesis explains, why a pet's location qualifies as personal data, how this information is technically accessed, and which legal instruments regulate the use of this data. In addition, the first part addresses how the basic data protection principles and the obligation to acquire an individual's consent create limitations regarding the use of the collected data. Furthermore, it is argued in the second part of this thesis that the real value of personal data to an enterprise is connected to the possibilities of third party data disclosure. In addition, it is argued that the European data protection rights, specifically the right to be forgotten and the right to data portability, significantly limit the app developer's potential to economically benefit from the collected location data. In this regard, the second part also includes forming a model to transfer location data in a private corporate acquisition process. The main research method used in this thesis is problem-oriented legal dogmatics and the main legal context is the European data protection framework.

The findings of this research are divided into two distinct arguments. *Firstly*, it is concluded that while rendering the collection of pets' location data lawful, the app developer should not over-value an end user's consent by considering it the sole sufficient basis to protect the fundamental rights and freedoms of the individual. *Secondly*, in the modern personal data economy, the app developer should treat personal information as a hybrid legal concept which effectively adapts itself to changing data protection situations. By including the end users to the data collection operations, the app developer also increases its own possibilities to profit from the personal information.

Keywords: data protection, location data, mobile application

Tiivistelmä

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta
VILPONEN, PAULIINA: Does locating pets qualify as processing of personal data?
Pro gradu -tutkielma, 80 s.
OTMU2247 Varallisuusoikeus ja taloudellisen toiminnan muutokset
Kesäkuu 2018

Sijaintitietojen kerääminen lemmikkieläimille tarkoitettujen elektronisten kaulapantojen avulla on uudenlainen henkilötietojen käsittelyn muoto. Teknisesti kyseisten sijaintitietojen kerääminen toteutetaan mobiililaitteelle asennettavan mobiiliapplikaation avulla. Kerättävät lemmikkieläinten sijaintitiedot linkittyvät eläinten omistajien tai muiden henkilöiden sijainteihin. Siksi mobiiliapplikaatiota operoivan tuotekehittäjän on noudatettava soveltuvaa tietosuojalainsäädäntöä.

Tämän tutkielman ensimmäisessä osassa selvitetään, miksi lemmikin sijaintitieto luetaan henkilötiedoksi, miten kyseinen tieto teknisesti kerätään ja mikä lainsäädäntö rajoittaa tiedon keruuta. Lisäksi ensimmäisessä osassa tarkastellaan, miten henkilötiedon käsittelyä koskevat perusperiaatteet sekä vaatimus hankkia rekisteröidyn suostumus rajoittavat sijaintitiedon käyttöä. Tämän tutkielman toisessa osassa puolestaan määritellään, kuinka henkilötiedon todellinen arvo yritykselle perustuu mahdollisuuksiin siirtää tieto edelleen kolmansille osapuolille. Toisessa osassa määritellään myös, kuinka rekisteröidyn henkilötiedon käsittelyä koskevat oikeudet rajoittavat mobiiliapplikaation kehittäjän mahdollisuuksia taloudellisesti hyötyä kerätystä sijaintitiedosta. Erityisesti oikeus tulla unohdetuksi ja oikeus siirtää tiedot järjestelmästä toiseen ovat tässä yhteydessä merkityksellisiä. Toiseen osaan kuuluu lisäksi osio, jossa luodaan malli sijaintitiedon siirtämiseksi yrityskaupan osana. Koko tutkielman tärkein tutkimusmetodi on ongelmakeskeinen lainoppi ja tärkein oikeudellinen kehys on eurooppalainen tietosuojalainsäädäntö.

Tutkielman tutkimustulokset voidaan tiivistää kahdeksi pääargumentiksi. Ensimmäisen argumentin mukaan mobiiliapplikaation kehittäjä ei saa yliarvioida rekisteröidyltä saadun suostumuksen merkitystä lemmikkieläimen sijaintitiedon lainmukaisen keräämisen yhteydessä. Kyseisestä yliarvioinnista on kysymys esimerkiksi silloin, jos suostumusta pidetään ainoana riittävänä perusteena rekisteröidyn oikeuksin ja vapauksien suojaamiseksi. Toinen argumentti puolestaan pohjautuu väitteelle, jonka mukaan nykyaikaisessa henkilötietojen vaihdannassa henkilötiedon määritelmä on alati muuttuva hybridi. Sallimalla loppukäyttäjilleen todellisen mahdollisuuden osallistua henkilötietojen keräämiseen ja käsittelyyn mobiiliapplikaation kehittäjä samalla lisää tiedon arvoa itselleen.

Avainsanat: tietosuoja, sijaintitieto, mobiiliapplikaatio

Contents

References

Literature

Andreansson, Ari – Koivisto, Juha – Ylipartanen, Arto. Tietosuojakäsikirja johdolle. Tietosanoma Oy 2015.

Beyleveld, Deryck – Brownsword, Roger. Consent in the Law. Hart Publishing 2007.

Blanchette, Jean-François. Burdens of Proof: Cryptographic Culture and Evidence in the Age of Electronic Documents. MIT Press cop. 2012.

Bygrave, Lee Andrew. Data Privacy Law: An International Perspective. Oxford University Press Online Version 2014.

Carey, Peter. Data Protection. A Practical Guide to UK and EU Law. Fourth Edition. Oxford University Press 2015.

Crilly, William M. – Sherman, Andrew J. The AMA Handbook of Due Diligence. American Management Association 2010.

Crompvoets, Joep – Janssen, Katleen. Geographic Data and the Law: Defining New Challenges. Leuven University Press 2012.

Gaughan, Patrick A. Mergers, Acquisitions, and Corporate Restructurings. Wiley 2010.

González Fuster, Gloria. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer 2014.

Katramo, Mikko – Lauriala, Jari – Matinlauri, Ismo – Niemelä, Jaakko E. – Svennas, Karin – Wilkman, Nina. Yrityskauppa. Sanomapro online version. Sanoma Pro Oy 2013.

Klitou, Demetrius. Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century. Springer 2014.

Kosta, Eleni. Consent in European Data Protection Law. Martinus Nijhoff Publishers 2013.

Landes, William M. – Posner, Richard A. The Economic Structure of Intellectual Property Law. Harvard University Press 2009.

Manson, Neil – O'Neill, Onora. Rethinking informed consent in bioethics. Cambridge University Press 2007.

Pöyhönen, Juha. Uusi varallisuusoikeus. Kauppakaari Oyj, Lakimiesliiton Kustannus 2000.

Saarnilehto, Ari – Annola, Vesa – Hemmo, Mika – Karhu, Juha – Kartio, Leena – Tammi-Salminen, Eva – Tolonen, Juha – Tuomisto, Jarmo – Viljanen, Mika. Varallisuusoikeus. Sanomapro online version. Sanoma Pro Oy 2001-2017.

Wilhelmsson, Thomas. Senmodern ansvarsrätt. Privaträtt som redskap för mikropolitik. Kauppakaari, Juristförbundets Förlag 2001.

Witzleb, Normann. Emerging Challenges in Privacy Law: Comparative Perspectives. Cambridge University Press 2014.

Articles

Aarnio, Aulis. Lainoppi. In *Mattila, Heikki E.S. (edit.)*. Encyclopaedia Iuridica Fennica VII: suomalainen oikeus-tietosanakirja. Suomalainen lakimiesyhdistys 1999, p. 331 – 338.

Aava, Ott. Risk Allocation Mechanisms in Merger and Acquisition Agreements. In Helsinki Law Review 2010/2, p. 31 – 59.

Aukia, Jussi-Pekka. GDPR-asetus tulee – entä sen jälkeen? In Lakimies 3/2018, p. 11 – 13.

Brownsword, Roger. The Cult of Consent: Fixation and Fallacy. In 15 King's Law Journal 2004, p. 223 – 251.

Bräutigam, Tobias JD. Getting high on Information? In JFT 5/2012, p. 415 – 435.

Chen, Liang – Thombre, Sarang – Järvinen, Kimmo – Lohan, Elena Simona – Alén-Savikko, Anette – Leppäkoski, Helena – H. Bhuiyan, M. Zahidul – Bu-Pasha, Shakila – Nunzia Ferrara, Giorgia – Honkala, Salomon – Lindqvist, Jenna – Ruotsalainen, Laura – Korpisaari, Päivi – Kuusniemi, Heidi. Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. In Special Selection on Security and Privacy in Applications and Services for Future Internet of Things. IEE Access, 5, 2017, p. 8956 – 8977.

Fredman, Janne. Tietosuoja-asioissa uusia velvoitteita myös pk-yrityksille. In Summa 3/2017, p. 8 – 10.

Hildebrandt, Mireille. Location Data, Purpose Binding and Contextual Integrity: What's the Message? In *Floridi, Luciano (edit.)*. Protection of Information and the Right to Privacy – A New Equilibrium? Springer 2014, p. 31 – 62.

Ismail, Noriswadi. Technology and 'Actors' in Data Protection. In *Ismail, Noriswadi – Lee, Edwin – Cieh, Yong*. Beyond Data Protection. Strategic Case Studies and Practical Guidance. Springer 2013, p. 99 – 110.

Kallasvuo, Karoliina. Omadata ja oikeus siirtää tiedot järjestelmästä toiseen. In *Korpisaari, Päivi (edit.)*. Oikeus, tieto ja viesti – Viestintäoikeuden vuosikirja 2015. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2016, p. 140 – 162.

Kangas, Urpo. Minun metodini. In *Häyhä, Juha (edit.)*. Minun metodini. WSOY 1997, p. 90 – 109.

Koski, Saara. Lasten henkilötietojen suojan tehokkuus ja riittävyys Euroopan unionissa – erityisesti esineiden internetin sovelluksissa. In *Korpisaari, Päivi (edit.)*. Viestinnän muuttuva sääntely – Viestintäoikeuden vuosikirja 2016. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2017, p. 33 – 67.

Korenhof, Paulan – Ausloos, Jef – Szekely, Ivan – Ambrose, Meg – Sartor, Giovanni – Leenes, Ronald. Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data. In *Gutwirth, Serge – Leenes, Ronald – Hert, Paul de (edit.)*. Reforming European Data Protection Law. Springer 2015, p. 171 – 202.

Kremer, Jens. The New EU General Data Protection Regulation: Setting Standards for the Next Century. In Liikejuridiikka 2016/2, p. 133 – 141.

Lauriala, Jari. Due Diligence in High-Tech M&A's. Edilex Article 2006.

Markou, Christiana. The 'Right to Be Forgotten': Ten Reasons Why It Should Be Forgotten. In *Gutwirth, Serge – Leenes, Ronald – Hert, Paul de (edit.).* Reforming European Data Protection Law. Springer 2015, p. 203 – 226.

Mäkelä, Joni. Virhevastuu yrityskaupoissa erityisesti ostajan suorittaman due diligence – tarkastuksen näkökulmasta tarkasteltuna. In Acta Legis Turkuensia 1/2011, p. 110 – 132.

Mäkinen, Jenni. The Personal Data Economy – From Black and White to Shades of Grey. In *Tiilikka, Päivi (edit.)*. Sananvapaus puntarissa – Viestintäoikeuden vuosikirja 2013. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2014, p. 174 – 202.

Nevasalo, Terho – Parviainen, Ella. Vuosi aikaa valmistautua EU:n uuteen tietosuoja-asetukseen. In Tilisanomat 3/2017, p. 28 – 31.

Ollila, Riitta. Henkilötietojen suoja EU:n perusoikeutena. Artikkeleita Eurooppaoikeudesta. In Defensor Legis 5/2014, p. 814 – 824.

O'Malley, Kate. "Too Many Eyes in the Sky": The Impact of Private Sector Drone Use on the Right to Privacy and Data Protection. In Helsinki Law Review 2015, p. 7 – 24.

Sartor, Giovanni. The Right to be Forgotten: Dynamics of Privacy and Publicity. In *Floridi, Luciano (edit.).* Protection of Information and the Right to Privacy – A New Equilibrium? Springer 2014, p. 1 – 16.

Schwartz, Paul M. Property, Privacy, and Personal Data. In Harvard Law Review 2004, Volume 117, Number 7, p. 2055 – 2128.

Tarhonen, Laura. Pseudonymisation of Personal Data According to the General Data Protection Regulation. In *Korpisaari, Päivi (edit.)*. Viestinnän muuttuva sääntely – Viestintäoikeuden vuosikirja 2016. Forum Iuris, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja 2017, p. 10 – 32.

Wilhelmsson, Thomas. Sosiaalisen siviilioikeuden metodiset lähtökohdat. In *Häyhä, Juha (edit.).* Minun metodini. WSOY 1997, p. 339 – 358.

Legislation

European Union

Charter of Fundamental Rights of the European Union, 2012/C 326/02.

Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('the Data Protection Directive'), 95/46/EC.

Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector ('the ePrivacy Directive'), 2002/58/EC.

Directive of the European Parliament and of the Council amending Directive 2003/98/EC on the re-use of public sector information, 2013/37/EU.

Proposal of the European Commission for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('the Proposal for the General Data Protection Regulation'), COM(2012) 11 final.

Proposal of the European Commission for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('the ePrivacy Regulation'), COM(2017) 10 final.

Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC ('the General Data Protection Regulation'), (EU) 2016/679.

Official references

European Commission

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century, COM(2012) 9 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "Building a European Data Economy", COM(2017) 9 final.

EU publication. *De Terwangne, Cécile.* The Right to be Forgotten and the Informational Autonomy in the Digital Environment. European Union 2013.

Korff, Douwe. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Country studies – A.4 Germany. The European Commission, Directorate-General Justice, Freedom and Security 2010.

Recommendation concerning the definition of micro, small and medium-sized enterprises, C(2003) 1422.

European Parliament

Report on the Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Report on the General Data Protection Regulation), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

The Future of Privacy – Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN, WP 168 (1 December 2009).

Guidelines on Consent under Regulation 2016/679, 17/EN, WP259 (28 November 2017).

Guidelines on the right to data portability 242 rev.1/2016, 16/EN, WP 242 rev.1 (13 December 2016, revised 5 April 2017).

Opinion 10/2004 on more harmonised information provisions, 11987/04/EN, WP 100 (25 November 2004).

Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136 (20 June 2007).

Opinion 13/2011 on geolocation services on smart mobile devices, 881/11/EN, WP 185 (16 May 2011).

Opinion 15/2011 on the definition of consent, 01197/11/EN, WP 187 (13 July 2011).

Opinion 02/2013 on apps on smart devices, 00461/13/EN, WP 202 (27 February 2013).

Working Document on the processing of personal data relating to health in electronic health records (EHR), 00323/97/EN, WP 131 (15 February 2007).

Court Decisions

Court of Justice of the European Union

Joines cases C-414/99, C-415/99 and C-416/99, *Zino Davidoff SA v A & G Imports Ltd and Levi Strauss & Co. v. Tesco Stores Ltd*, (2001) ECR I-8691.

Case C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596.

Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, ECLI:EU:C:2008:727.

Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR/Hartmut Eifert v. Land Hessen*, (2010) ECR I-11063. Including Opinion of the Advocate General Sharpston delivered on 17 June 2010.

Case C-131/12, *Google Spain v. Agencia Espanola Protección de Datos and Mario Costeja González*, ECLI:EU:C:2014:317.

European Court of Human Rights

Case 35623/05, *Uzun v. Germany*, 2 December 2010.

Internet references

Aalto-Setälä, Minna. EU:n tietosuoja-asetus tulee – valmistaudu ajoissa. Chamber of Commerce of Finland. Available at: http://kauppakamari.fi/2016/03/31/eun-tietosuoja-asetus-tulee-valmistaudu-ajoissa/ (27 March 2017).

Bapat, Anita. The new right to data portability. Privacy & Data Protection, Volume 13, Issue 3. Available at: https://www.hunton.com/images/content/3/1/v2/3122/The_new_right_to_data_portability_Bapat.pdf (8 April 2018).

Bird & Bird GDPR Guide. Bird & Bird LLP. Available at: https://www.twobirds.com/en/hot-topics/general-data-protection-regulation/download-guide-by-chapter-topic (27 March 2017).

Bertram, Theo – Bursztein, Elia – Caro, Stephanie – Chao, Hubert – Chin Feman, Rutledge – Fleischer, Peter – Gustafsson, Albin – Hemerly, Jess – Hibbert, Chris – Invernizzi, Luca – Kammourieh Donnelly, Lanah – Ketover, Jason – Laefer, Jay – Nicholas, Paul – Niu, Yuan – Obhi, Harjinder – Price, David – Strait, Andrew – Thomas, Kurt – Verney, Al. Three years of the Right to be Forgotten. Google. Available at: https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK/view (1 April 2018).

Bluetooth. Bluetooth Technology – Radio Version. Available at: https://www.bluetooth.com/bluetooth-technology/radio-versions (4 March 2018).

Business Dictionary. Definition of '*end user*'. Available at: http://www.businessdictionary.com/definition/end-user.html (4 December 2017).

Business Dictionary. Definition of '*privacy policy*'. Available at: http://www.businessdictionary.com/definition/privacy-policy.html (4 December 2017).

Business Dictionary. Definition of '*startup*'. Available at: http://www.businessdictionary.com/definition/startup.html (23 March 2017).

Curtis, Sophie. How much is your personal data worth? The Telegraph. Available at: https://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html (28 March 2018).

Cambridge Dictionary. Definition of '*public*'. Available at: https://dictionary.cambridge.org/dictionary/english/public (4 April 2018).

Chapman, Jon. Warranties, Representations and Indemnities. ClarksLegal. Available at: https://www.clarkslegal.com/Blog/Post/Warranties_Representations_and_Indemnities_ (20 June 2018).

The European Commission. Adequacy decisions. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu (1 April 2018).

Financial Dictionary. Definition of '*M&A*'. Available at: https://financial-dictionary.thefreedictionary.com/M%26A (9 April 2018).

Financial Dictionary. Definition of '*vertical acquisition*'. Available at: https://financial-dictionary.thefreedictionary.com/Vertical+acquisition (9 April 2018).

Gabel, Detlev Dr. – Hickman,Tim. Chapter 7: Lawful basis for processing – Unlocking the EU General Data Protection Regulation. White & Case LLP. Available at: https://www.whitecase.com/publications/article/chapter-7-lawful-basis-processing-unlocking-eu-general-data-protection (27 March 2017).

Google. Google Transparency Report. Available at: https://transparencyreport.google.com/eu-privacy/overview?delisted_urls=start:1401321600000;end:1519862399999&lu=delisted_urls (30 March 2018).

Howard, Philip N. – Gulyas, Orsolya. Data breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014. Center for Media, Data and Society. Available at: https://poseidon01.ssrn.com/delivery.php?ID=442100001087089097003100095101098126033069042014023087069030080022115002096001122121107056043003059006011085112122004001076001098001090058041022067125102097084076086055054002072089115087004021113121090028125093071003083080098113117068101074071117104126&EXT=pdf (30 March 2018).

Ilan, Daniel. Privacy in M&A Transactions: Pre Closing Liabilities. Harvard Law School Forum on Corporate Governance and Financial Regulation. Available at: https://corpgov.law.harvard.edu/2016/11/07/privacy-in-ma-transactions-pre-closing-liabilities/ (4 December 2017).

Ilan, Daniel. Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities. Harvard Law School Forum on Corporate Governance and Financial Regulation. Available at: https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/ (24 April 2018).

Kelley, Diana. Is Bluetooth Security Good Enough for Your Most Sensitive Corporate Communications? Security Intelligence. Available at: https://securityintelligence.com/is-bluetooth-security-good-enough-for-your-most-sensitive-corporate-communications/ (5 March 2018).

Lindroos, Anette – Walkjärvi, Annamari. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman. Available at: http://www.castren.fi/blogandnews/blog-2016/how-to-take-data-protection-into-account-in-ma-transactions--6-tips/ (10 April 2018).

Long, William – Shankar, Vishnu. The impact of the GDPR on the retention of personal data. International Association of Privacy Professionals (IAPP). Available at: https://iapp.org/media/pdf/resource_center/GDPR-retention-sidley-september-2016-1516.pdf (17 January 2018).

Marr, Bernard. Why Data Minimization is an Important Concept in the Age of Big Data. Forbes. Available at: https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/2/#2df797e4c245 (15 January 2018).

Maxwell, Winston – Parsons, Mark – Loughlin, Scott T. – Schreibauer, Marcus – Taied, Sarah. Data protection in M&A transactions: A how-to-guide. Hogan Lovells. Available at: http://www.hoganlovells.com/files/upload/10358_EUn_GMCQ%20Autumn%202_2015_E.pdf (11 April 2018).

Merriam-Webster Dictionary. Definition of '*redaction*'. Available at: https://www.merriam-webster.com/dictionary/redact (11 April 2018).

Merrill Corporation. What Is a Virtual Data Room (VDR)? Available at: https://www.merrillcorp.com/en/glossary/virtual-data-room (10 April 2018).

Moreno, Hugo. The Importance of Data Quality – Good, Bad or Ugly. Forbes. Available at: https://www.forbes.com/sites/forbesinsights/2017/06/05/the-importance-of-data-quality-good-bad-or-ugly/#9b181fe10c4d (16 January 2018).

Oxford Dictionary. Definition of '*geolocation*'. Available at: https://en.oxforddictionaries.com/definition/geolocation (4 December 2017).

ShareVault (Pandesa Corporation). How to redact text or images in a PDF. Available at: https://www.sharevault.com/resources/glossary/how-to-redact (11April 2018).

Steel, Emily – Locke, Callum – Cadman, Emily – Freese, Ben. How much is your personal data worth? Financial Times. Available at: https://ig.ft.com/how-much-is-your-personal-data-worth/ (28 March 2018).

Titcomb, James. 'Facebook is listening to me': Why this conspiracy theory refuses to die. The Telegraph. Available at: http://www.telegraph.co.uk/technology/2017/10/30/facebook-listening-conspiracy-theory-refuses-die/ (30 January 2018).

The UK Information Commissioner's Office. Location data in brief. Available at: https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/ (11 October 2017).

Updated Legal Terms. Facebook. Available at: https://www.facebook.com/legal/terms/update (28 March 2018).

Warma, Eija. Finally Agreed – New Data Protection Regulation Is Here! Castrén & Snellman. Available at: http://www.castren.fi/blogandnews/news-2016/finally-agreed---new-eu-data-protection-regulation-is-here/ (22 March 2017).

Abbreviations

API	Application Programming Interface
App	Mobile application
Board	European Data Protection Board
Court	Court of Justice of the European Union
Directive	Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data
ePrivacy Directive	Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector
EU	European Union
GMS	Global System for Mobile Communications
GPS	Global Positioning System
Ibid.	Ibidem, in the same place
IoT	Internet of Things
OS	Operating System
Regulation	Regulation of the European Parliament and the Council 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
WiFi	Wireless local area networking
Working Party	Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. Introduction

1.1. Finding the context

"*Imagine that every person who posts information on the Internet or on other communication platforms would have to acquire the consent of everybody he is referring to, as stricto sensu*[1] *he is processing their personal data*."
– *Eleni Kosta*. Consent in European Data Protection Law.

Personal data is information that *relates to an identified or identifiable natural person*. In this context, the term *identifiability* refers to the combination of unique, case-specific factors that result in the final identification. The identification can be direct or indirect, but in either case it should be based on an *identifier* such as a name or location data.[2] The most common *direct identifier* is a person's name.[3] Occasionally, the name would need to be combined with additional information to clearly distinguish a single person from other individuals. In doing so, an *indirect identifier* is established by combining two or more details such as name, age, and location information. In the context of personal data, someone is considered *unidentifiable* if all reasonable means do not suffice to identify the natural person.[4] In this thesis, the term *personal data* is used to refer to any direct or indirect identifier.

Personal data *relates to a natural person* when it is generally about an individual. The specific content, purpose or result of the data usage indicates whether the necessary link is established. The definition is not restrictive and can include almost all information concerning identifiable individuals.[5] For example, information contained in the results of a medical analysis or in a phone call log usually qualifies as personal data.[6] In addition, professional habits and practices, video surveillance footage, as well as information related to private and family life are less common examples of personal data. The above information can be objective or subjective, and does not need to be true

[1] In the strict sense.
[2] Article 4(1) of the Regulation.
[3] *Nevasalo and Parviainen* 2017, p. 29.
[4] Opinion 4/2007 of the Working Party, p. 12 – 17.
[5] Ibid., p. 4.
[6] Ibid., p. 9 – 12.

or proven.[7]

Processing of personal data is a comprehensive concept including various operations performed on personal information.[8] For example, processing might consist of collection, recording, organisation, structuring, storage, and erasure.[9] One noteworthy and unconventional form of data processing is accessing location information on an electronic collar worn by a pet. This kind of information reveals when and where the pet is moving, where it lives, and when it sleeps. Technically, the data would be accessed in the context of a mobile application operated on a mobile device. Both the electronic collar and the operating mobile device would be closely connected to the location of the mobile application's user. Therefore, all data collection and recording operations performed within the application would qualify as processing of personal data.

Data protection is a fundamental right of individuals, recognised both in national and international legislation.[10] According to Article 8 of the *Charter of Fundamental Rights of the European Union* (2012/C 326/02, the Charter of Fundamental Rights, later referred to as '*the Charter*'):

> "*Everyone has the right to the protection of personal data concerning him or her.*
>
> *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *Compliance with these rules shall be subject to control by an independent authority*."

[7] Ibid., p. 6 – 9.
[8] *Warma* 2015. Finally Agreed – New Data Protection Regulation Is Here! Castrén & Snellman.
[9] Article 4(2) of the Regulation.
[10] *González Fuster* 2014, p. 1 – 3.
In the case *Bodil Lindqvist* (C-101/01) the Court found that, for example, mentioning persons on the Internet qualifies as processing of personal data.
Furthermore, in the case *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* (C-73/07) the Court ruled that collecting, processing and publishing information relating to taxation qualifies as data processing.

1.2. Defining the research

This thesis focuses on the problems posed by processing personal data in the context of the mobile application (later referred to as '*the app*') offering the *geolocation*[11] services to pet owners (later referred to as '*the end user(s)*'[12]). The app collects the location data transmitted by the electronic collars, and subsequently, by the operating mobile devices. A pet, such as a dog or cat, wears the electronic collar, and the end user accesses the transmitted information on his or her mobile device. The specific functions of the app include tracking pets' activity, monitoring their moving patterns, and following their daily sleeping behaviour. The app also registers whether the pets' activity is minimal, balanced, rhythmic, or high energy. The electronic collars collect location data using the GMS, GPS, and WiFi infrastructures. Next, the collected information is transmitted to the operating mobile devices using the Bluetooth and WiFi technologies. If the electronic collars cannot detect a Bluetooth or WiFi connection, they then store the tracking information up to 30 days. Once reconnected, the collars automatically synchronize the previously collected data. In the case of no direct connection between a collar and mobile device, the end users may also track their pets using the GPS infrastructure. In addition to the collection of location data, the electronic collars contain sensors for warmth and brightness, as well as an accelerometer for the purposes of measuring activity levels as mentioned above.

In order to facilitate smooth operation of the geolocation services, the operating mobile devices must allow the app to access information on their hardware and make use of their operating systems.[13] This means that the mobile devices manage the operation of the app through the Application Programming Interfaces (later referred to as '*the APIs*'). In general, the APIs are technology built into the devices to ensure smooth access of their various sensors. These sensors include the gyroscope, digital compass, accelerometer, as well as front and rear cameras. In addition, fundamental components, such as the address book, are accessible. In the context of this thesis, the APIs enable access to the mobile devices' location data collected within the GMS, GPS and WiFi

[11] According to Oxford Dictionary, '*geolocation*' is the process or technique of identifying the geographical location of a person or device.
[12] According to Business Dictionary, '*end user*' is a person or organisation that uses a product, as opposed to the person or organisation that authorises, orders, procures, or pays for it.
[13] Opinion 2/2013 of the Working Party, p. 4.

infrastructures, similarly to the electronic collars.[14]

The first part of this thesis focuses on two research questions. *Firstly*, this thesis explains, why information related to a pet's location qualifies as personal data, how this information is technically accessed, and which legal instruments regulate the use of this data. *Secondly*, this thesis addresses how the basic data protection principles as well as the obligation to acquire an end user's consent create limitations regarding the use of the collected data. The main research method is *practical legal dogmatics*[15] and the main legal context is the current European data protection framework (later referred to as '*the data protection framework*'). This context is chosen due to the general focus of the current legal research.[16] The data protection framework is approached pragmatically, and the legal instruments, mainly *the Regulation of the European Parliament and of the Council 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* ((EU) 2016/679, the General Data Protection Regulation, later referred to as '*the Regulation*'), are reflected against the increasing use of mobile devices. The research method used is further specified as *problem-oriented legal dogmatics*, meaning that the data protection framework is analysed and systemised in relation to a practical problem, data processing within the app.[17]

The second part of this thesis is based on two further research questions. *Firstly*, it is argued that the real value of location data to an enterprise is connected to the possibilities of third party data usage. In this regard, the data protection rights granted to individuals in the Regulation, specifically the right to be forgotten and the right to data portability, significantly limit the app developer's potential to economically benefit from the collected information. *Secondly*, a model is formed to address the challenge of transferring location data in a private corporate acquisition process.[18] As usual in the context of the apps, it is presupposed that the app developer is a small or medium-sized *startup* company. '*Startup*' can be defined as the "*early stage in the life cycle of an enterprise where the entrepreneur moves from the idea stage to securing financing,*

[14] Ibid.
[15] According to *Aarnio* 1999 (p. 334), the purpose of legal dogmatics is to interpret legal clauses.
[16] *Chen and others* 2017, p. 8958.
[17] *Kangas* 1997, p. 93 – 109.
[18] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Harvard Law School Forum on Corporate Governance and Financial Regulation.

laying down the basic structure of the business, and initiating operations or trading".[19] For the startup company, the collected location data creates a fundamental economic asset in its business operations. Subsequently, prudent data protection increases the value of the asset and makes it tradeable in a private corporate acquisition process. It is normal for the budding startup company to be at some point acquired by an industrial buyer or private equity investor. Therefore, addressing the problem of the data flows in an acquisition process is necessary to the above specified research questions.[20] In this second part, the method used is a combination of practical (problem-oriented) legal dogmatics and *social civil law*. The method of social civil law reflects the perception that law and justice provide the opportunity to create various interpretations and moral choices. The method is used mainly in the thesis conclusions and propositions, contributing to the development of the data protection framework.[21]

In this thesis, the Regulation is the main legislative source of reference. As it is a new component of the data protection framework, studies that have been conducted concerning the former European data protection legislation might be outdated. However, studies that regard the former *Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (95/46/EC, the Data Protection Directive, later referred to as '*the Directive*') are applicable in parts, where no material changes have occurred. Therefore, the opinions of the *Working Party on the Protection of Individuals with regard to the Processing of Personal Data* (later referred to as '*the Working Party*'), set up in Article 29 of the Directive, are often used. The Working Party was an independent advisory body that addressed questions regarding the protection of individuals' personal data. It was comprised of one representative from every Member State's Data Protection Authority, one representative from the EU institutions, and one representative from the European Commission.[22] In the Regulation, the Working Party has been substituted with the *European data protection board* (later referred to as '*the Board*'), set up in Chapter VII Section 3. The Board is also an independent body of the European Union (later referred to as '*the EU*') consisting of the

[19] Business Dictionary. Definition of '*startup*'.
[20] *Lauriala* 2013, Chapter 1.1 Yristysostajat. Sanomapro online version.
[21] *Wilhelmsson* 1997, p. 339 – 355.
[22] *Carey* 2015, p. 9 – 10.

head of a supervisory authority of each Member State and of the European Data Protection Supervisor.[23]

[23] Recital 139 of the Regulation.

2. Basic data protection principles and consent to the processing of pets' location data

2.1. Location data

2.1.1. Definition of location data

Continuous collection of pets' location data is a fundamental characteristic of the app. *Primarily*, the app would access location data transmitted by the electronic collars enabling it to form the specific movement patterns over time. *Secondarily*, the app would process location data transmitted by the operating mobile devices. This information would be necessary to track a missing pet using the GPS infrastructure and to determine the distance between a mobile device and electronic collar. Even if the app does not access location data on the operating mobile device, the location of the electronic collar is still normally connected to the end user or another person. Subsequently, this Sub-Chapter elaborates why the app should treat all collected location information as personal data of the end users.

According to the Regulation, information on location is an identifier of personal data.[24] Generally, location data means information about the location of a mobile or other device, and subsequently, of a natural person.[25] In detail, location data is defined in Article 2(c) of the *Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector* (2002/58/EC, later referred to as '*the ePrivacy Directiv*e'), being any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user[26] of a publicly available electronic communications service. According to Recital 14 of the ePrivacy Directive, location data is information connected to the latitude, longitude and altitude of a user's terminal equipment. In addition, it may indicate travel direction, level of locating accuracy, time of locating, or network cell where the terminal equipment is located.

[24] Article 4(1) of the Regulation.
[25] UK Information Commissioner's Office's website. Location data in brief.
[26] According to Article 2(a) of the ePrivacy Directive, "*user means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service*".

Following the acquisition of location data, further personal information may be revealed. This further data is formed by accumulating ongoing location information or by identifying information connected to a specific location. For example, location data may reveal a person's home address, place of work, health condition, or political opinion.[27]

Originally, location information was identified as personal data due to the massive role that mobile devices have in our everyday lives. In the context of the app, the privacy settings of a mobile device could enable the app developer to deduct very private information on an individual's daily habits and collect data on his or her routine movement patterns.[28] This collection could be indirectly conducted as a pet normally reside close to the end user or another person. Only occasionally, the pet might go outside alone or stay in a kennel for a short period of time. Therefore, to avoid illegal processing of personal data, all location information acquired in the context of the app should be treated as personal data.

As further reasoning for the above conclusion, the definition of location data can be further specified by elaborating the definition of data processing. In this regard, the *Court of Justice of the European Union* (later referred to as '*the Court*') set forth in the case *Google Spain v Agencia Espanola de Protección de Datos and Mario Costeja Gonzaláles* that the operations of online search engines constitute processing of personal data. The search engine enterprises, like in the case *Google Spain*, search the internet constantly and systematically to find published information for the purposes of answering user requests. The search results might include information that qualifies as personal data, and therefore, the entire collection is categorised as data processing. In the context of a search, it is impossible to differentiate between personal data and other information.[29]

Like a search engine operator, also the app developer collects data constantly and systematically to provide information to the end users.[30] In the context of pet monitoring, the app developer is not able to identify when the collected data connects to

[27] *Kosta* 2013, p. 379 – 380.
[28] Opinion 13/2011 of the Working Party, p. 7.
[29] Case C-131/12 of the Court, p. 10.
[30] Ibid.

the location of identifiable natural persons. In practice, there is only a marginal chance that the data would not be connected to any individual. For example, this would be the case if a pet enters into a fully automated warehouse used solely by machines[31] or walks alone in the middle of a forest. Here, the mere information that the end user is not within the range of the electronic collar does not amount in identifiable personal data. However, ongoing locating could reveal over time that the end user almost never resides close to the pet, and therefore, omits taking care of it. In doing so, the accumulated information would qualify as personal data. Due to this conclusion, the app developer is not able to determine that in some cases the collected location data is not personal data. Subsequently, all data collection carried out within the app amounts in processing of personal data.

2.1.2. Infrastructures enabling access to location data

In order to specify how the data protection framework regulates the collection of pets' location data within the app, it is essential to understand how the app accesses location data within the relevant locating infrastructures. In addition, it is fundamental to identify the risks connected to the locating. Technically, many different infrastructures could enable the app to determine the location of the electronic collars and the operating mobile devices. However, the relevant locating infrastructures specified in the introduction to this thesis are GMS (Global System for Mobile Communications), GPS (Global Positioning System), and WiFi (wireless local area networking).[32]

The GSM base stations constitute an infrastructure commonly used by the telecommunication operators to determine the location of mobile devices. Within this infrastructure, each operator covers a specific area divided into one or more cells. The geographic size of the cells varies and depends on the type of the covered area. Densely populated cities with high buildings are divided into smaller cells than open and sparsely populated rural areas. Each cell has a base station which connects with smart devices. Using the technique called *triangulation*, the operators can combine signals from multiple base stations, and subsequently, increase the accuracy of locating. In addition, the techniques called RSSI (Received Signal Strength Indicator), TDOA

[31] *Janssen and Crompvoets* 2012, p. 98.
[32] Opinion 13/2011 of the Working Party, p. 3.

(Time Difference of Arrival) and AOA (Angle of Arrival) offer further accuracy. Within the app, locating using the GSM base stations is not very precise in comparison to the GPS and WiFi infrastructures. The accuracy of the infrastructure ranges from 50 meters to several kilometres.[33]

The GPS infrastructure enables locating by 31 different satellites transmitting radio signals. When a mobile or similar smart device captures at least four of the signals concerned, it can determine its relatively precise location. Unlike the operators using information from the GSM base stations, the GPS infrastructure operators are not able to identify which devices have received or are receiving radio signals from the satellites. The identification is impossible as the transmitted GPS radio signals only go one way, from the satellites to the devices.[34] For this reason, *O'Malley* has argued that devices which use the GPS technology, such as drones, are less privacy intrusive than for example video and voice surveillance.[35] Despite the precision of GPS locating (from 4 to 15 meters), the infrastructure does not offer fluent operation indoors and takes longer to start than services based on other infrastructures. In the context of the app, the GPS infrastructure is normally used in combination with the GSM or WiFi infrastructures.[36]

The WiFi infrastructure is divided into numerous local access points. Each access point has a unique ID, a MAC (Medium Access Control) address. The specific MAC address of a WiFi access points is called BSSID (Basic Service Set Identifier), and in addition, MAC addresses are recorded in hardware of computers, phones, and other smart devices. The BSSID of an access point can be sent to a smart device and the smart device concerned can further transmit the ID to a service provider for the purposes of locating. Locating in the context of the WiFi infrastructure is possible on an ongoing basis as the access points announce their existence constantly. Moreover, WiFi locating does not require that the smart device is connected to the network or that the network is not encrypted (WEP, WPA, or WPA2). The BSSIDs can be collected either by active

---

[33] Ibid., p. 4.
[34] Ibid., p. 4 – 5.
[35] *O'Malley* 2015, p. 15.
In addition, the European Court of Human Rights has concluded in Paragraph 52 of the case *Uzun v. Germany* (35623/05) that "*GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions, or feelings*".
[36] Opinion 13/2011 of the Working Party, p. 4 – 5.

scanning (sending active requests and recording the answers) or by passive scanning (recording beacon frames transmitted by access points). Active scanning does not reveal the MAC addresses of the connected devices. On the contrary, passive scanning might do so, and subsequently, offer very detailed information on the devices. Normally, the service providers use the WiFi infrastructure dynamically, meaning that once allowed to do so, the smart devices repeatedly communicate all available access point and MAC address information. With this kind of data, the app developer can calculate the location of the relevant smart devices on an ongoing, precise basis.[37]

The risks associated with locating in the context of the GSM, GPS and WiFi infrastructures are multiple. The main risk within the app is the lack of transparency as many end users may not be aware of the technologies behind the locating techniques or their locating accuracy. Moreover, the app offers a *hybrid service* combining the GSM, GPS and WiFi infrastructures, and subsequently, the data collection is extremely accurate and sensitive in relation to the individuals. In this regard, poor security measures protecting the collected data can facilitate serious data breaches, and vague purpose limitations can cause unwanted spreading of location data.[38] As a fundamental protection for the end users' rights and freedoms, the data protection framework offers various legal obligations limiting the use of the data. These obligations are further addressed below.

2.1.3. Legal basis for the collection of location data

For the app developer, the general data protection obligations of the Regulation and Article 5(3) of the ePrivacy Directive together form the legal basis for the collection of pets' location data. In this regard, the obligations of the Regulation are the main legal basis. However, the Regulation is a piece of data protection legislation governing a general matter (*lex generalis*), and therefore, it is often overridden by sector specific legislation (*lex specialis*).[39] Therefore, the ePrivacy Directive applies to accessing information on the terminal equipment of the end users.[40]

---

[37] Ibid., p. 5 – 6.
[38] Opinion 02/2013 of the Working Party, p. 6.
[39] *Kosta* 2013, p. 277 – 278.
[40] Article 5(3) of the ePrivacy Directive.
The ePrivacy Directive is currently going through radical change. In 2017 the European Commission adopted a *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing*

In general, the ePrivacy Directive applies to the processing of personal data in the context of publicly available electronic communications services in public electronic communications networks.[41] This scope is relatively restrictive as the term '*publicly available*' excludes an extensive amount of data processing to which only the Regulation applies.[42] Concerning locating, the ePrivacy Directive mainly applies to data processing conducted by the telecommunication operators within the GSM infrastructure. Even if a telecommunication operator offers a hybrid service combining the GSM, GPS and WiFi data, the ePrivacy Directive applies to the entire service. However, if the provider of the hybrid service is not a telecommunication operator, but for example the app developer, the offered service is called *information society service*. By definition, the term '*electronic communications service*' does not include the information society service. Therefore, the ePrivacy Directive does not outright apply to the collection of pets' location data within the app. The rule stands even if the data collection is conducted via a public electronic communications network.[43]

According to Article 5(3) of the ePrivacy Directive (as amended by the Directive 2009/136/EC):

> "*The Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.*"

The consent requirement of this Article applies to all kinds of data processing independent of the processing entity. It applies even to data processing to which the ePrivacy Directive would not be applied otherwise. If information is accessed on the terminal equipment of a subscriber or user, the consent of the subscriber or user should be acquired before any access is made. As Article 5(3) makes no difference between personal data and other information, it does not require that the data on the terminal equipment is specified. According to the Working Party, location data is one type of

---

Directive 2002/58/EC (COM(2017) 10 final, the ePrivacy Regulation). This new Regulation should update the ePrivacy Directive to better fit the data protection framework.

[41] Article 3(1) of the ePrivacy Directive.

[42] *Kosta* 2013, p. 379 – 380.

[43] Opinion 13/2011 of the Working Party, p. 7 – 9.

information commonly accessed on the terminal equipment of a subscriber or user. If this kind of information is accessed, the requirements for valid consent stipulated in the Regulation should be respected as further addressed in Sub-Chapter 2.2.3..[44] Therefore, Article 5(3) of the ePrivacy Directive applies to the collection of location data within the app.

2.2. Lawful data processing according to the data protection framework

2.2.1. Actors of the data protection framework

Most of the obligations stipulated in the data protection framework are based on the relationship of a data subject and data controller.[45] In the meaning of the Regulation, the end users qualify as data subjects and the app developer qualifies as data controller. Before further addressing how the data protection framework regulates this legal relationship, it is crucial to determine the legal definition of data subject and data controller. In addition, it is essential to scrutinise which other entities process personal data in relation to the app, and in which way this factor affects the basic relationship.

In the Regulation, '*data subject*' means any identified or identifiable natural person[46], and '*data controller*' means a natural or legal person, public authority, agency, or any other body which *determines the purposes and means of the processing of personal data*. The purposes and means may be determined either alone or jointly with other data controllers. In addition, the EU and the Member States are authorised to adopt laws that set forth adequate purposes and means.[47] Generally, all sole traders, partnerships, and companies are likely to be data controllers.[48] The definition includes online and other businesses, such as banks, law firms, Internet search engines, and telecommunication businesses.[49] The data controllers are legally responsible for all data processing conducted under their control. They need to effectively demonstrate compliance with the data protection legislation[50] and implement appropriate technical and organisational

[44] Opinion 02/2013 of the Working Party, p. 7 – 8.
[45] *Ismail* 2013, p. 106.
[46] Article 4(1) of the Regulation.
[47] Article 4(7) of the Regulation.
[48] *Aukia* 2018, p. 11.
[49] *Carey* 2015, p. 29 – 30.
[50] *Ollila* 2014, p. 816.

measures to ensure lawfulness of data processing.[51] Most of the obligations set forth in the Regulation are directly applicable on the data controllers.[52]

According to Article 4(8) of the Regulation, '*data processor*' means a natural or legal person, public authority, agency, or any other body which processes personal data *on behalf of a data controller*. It is required in the Regulation that the data processor is contractually obliged by the data controller to comply with the data protection legislation in applicable parts.[53] Moreover, each sub-processor of the original data processor needs to be contractually obliged to comply with corresponding responsibilities. The above statement means that if the data protection obligations laid down in the data protection framework do not affect the data processor directly, they normally do so via contractual clauses.[54]

In practice, it might be difficult to distinguish whether an entity qualifies as data controller or data processor. Some entities wish to identify as data processor to avoid the compulsory application of specific data protection obligations. On the contrary, some entities prefer to identify as data controller to use the collected personal data for supplementary purposes such as for marketing of related services. The degree of autonomy defines the legal status of an entity. An organisation which conducts data processing on behalf of someone else and does not determine the purposes and means of the processing, qualifies as data processor.[55] As an example, cloud service suppliers are generally treated as data processors. The rule stands even if a specific supplier manages its contractual relationships by general standard terms of business. The use of the standard terms does not affect the data controller's legal responsibility to demonstrate compliance with the data protection legislation.[56]

In the context of the apps in general, the Working Party has identified four data controller/processor categories involved in the development, distribution and operation of the software.[57] The first category includes the app developers and app owners. An app developer is a person or entity which develops and operates an app. It normally

[51] *Witzleb* 2014, p. 68 – 69.
[52] *Carey* 2015, p. 261 – 268.
[53] *Aukia* 2018, p. 11.
[54] *Carey* 2015, p. 261 – 268.
[55] *Nevasalo and Parviainen* 2017, p. 29.
[56] *Carey* 2015, p. 266 – 267.
[57] Opinion 02/2013 of the Working Party, p. 9.

decides which categories of personal data are processed, how the data is collected, how it is stored, and how the app protects the information from third party data breaches[58]. In doing so, the app developer determines the purposes and means of the data collection and qualifies as data controller in the meaning of the Regulation. On the other hand, an app owner is a person or entity which has outsourced the development of an app, but still predominantly determines the purposes and means of the processing. Therefore, like the app developers, also the app owners qualify as data controllers.[59]

The second data controller/processor category are the Operating System (later referred to as '*the OS*') and device manufacturers. These entities manage the way various components and technology of smart devices are used. The OS and device manufacturers customise the APIs for the mobile devices, and subsequently, control the way the apps access information on their hardware. For example, the app developer providing the geolocation services must use a locating system supported by a specific OS. Legally, the OS and device manufacturers either process personal data only on behalf of the app developers and app owners or use the data also for their own purposes. In the first case, the manufacturers qualify as data processors. In the latter case, the manufacturers commonly are joint data controllers and jointly responsible (with an app developer or app owner) for the data processing. As an example, this kind of joint controllership is established if in addition to an original processing purpose personal data is used to improve the functionality of a manufacturer's services.[60]

The third data controller/processor category are the app stores. In order to download an app to a mobile device, an end user needs to visit an app store operated by an OS manufacturer. Before proceeding to the download, login is required to access a specific store. The login might obligate an individual to disclose personal information, such as name, address, phone number, and credit card details. In addition to the login credentials, the app store concerned might collect supplementary data, such as data on recently downloaded apps or on other similar activities. In the meaning of the Regulation, the app stores qualify as data controllers regarding the information they collect and process for their own purposes, such for the login process. Furthermore, they

[58] For more information on recorded data breaches in Europe: *Howard, Philip N. and Gulyas, Orsolya*. Data breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014.
[59] Opinion 02/2013 of the Working Party, p. 9 – 10.
[60] Ibid., p. 10 – 11.

qualify as joint data controllers for the cooperative data collection with the app developers and app owners. This is the case when information on an individual's online activity is used to personalise the app store experience and the app usage. If an app store does not use any personal information for its own purposes, it qualifies as data processor and offers a mere platform on which other parties can collect personal data.[61]

The fourth data controller/processor category includes every other third party that somehow processes personal data in relation to an app. Two examples of these third parties are the advertisers and analytics providers. The advertisers process personal data to provide personalised advertisements to app users. This task is fulfilled by using cookies[62] or similar tracking facilities.[63] Especially, if an app is downloadable free of charge, it is most probably financed by third party advertisements, creating the actual business opportunity for the relevant app developer.[64] In doing so, the collection of personal data is the price the users pay for using the app.[65] On the other hand, the analytics providers facilitate the app developers and app owners with information on how often and how much their app has been used. The analytics providers might also offer information on the apps' usability or on common functional problems. In general, the third parties are divided into two different groups. *Firstly*, the third parties might provide information requested by the app developers and app owners, and process the data only for this purpose as data processors. *In addition*, they might use the personal information for their own benefit, such as to avoid displaying same advertisements multiple times. In the latter case, the third parties qualify as single or joint data controllers.[66]

This thesis focuses on the relationship of the pet monitoring app and the end users. The app developer designs and deploys the app as well as is legally responsible for the data collection. In practice, the responsibility might be joint as the app is most probably bought from a specific app store offered by a specific OS manufacturer. Nevertheless,

---

[61] Ibid., p. 11 – 12.
[62] According to *Carey* 2015 (p.281), '*cookies*' are text files placed, among others, on the hard drive of a subscriber's or user's computer. The placement is conducted by website operators to recognise users revisiting specific sites. The cookies can be either permanent or temporary (session-cookies). In practice, they save settings on websites or transmit information on online activity.[62]
[63] Opinion 02/2013 of the Working Party, 12 – 13.
[64] *Mäkinen* 2013, p. 180 – 181.
[65] Ibid., p. 1 – 2.
[66] Opinion 02/2013 of the Working Party, p. 12 – 13.

these accumulating relationships are primarily left outside the scope of the research and the following Chapters mainly focus on the data protection obligations applicable on the app developer qualifying as the data controller.

2.2.2. Basic data protection principles

Compliance with the basic data protection principles[67] stipulated in Article 5 of the Regulation is the foundation of lawful data processing within the pet monitoring app. All other obligations established in the data protection framework are based on the principles, and therefore, their practical meaning is significant.[68] In addition, appropriate implementation of the basic principles ensures that the app developer comprehensively respects data protection as a fundamental right of the end users. The basic principles are (1) data minimisation, (2) data quality, (3) storage limitation, (4) purpose limitation, (5) integrity and confidentiality, (6) fairness and lawfulness, and (7) accountability.[69] In some cases, special exceptions might override the application of the principles. However, these exceptions are generally not relevant to the research questions of this thesis, and therefore, only the principles (1) – (6) are further addressed in the following Sub-Chapters.

In practice, the effective implementation of the basic principles is essential for the app developer due to two distinct factors. *Firstly*, Article 83 of the Regulation concerns administrative fines imposed on organisations infringing specific Articles of the Regulation. The administrative fines are divided into two levels based on the gravity of an infringement. In the case of an infringement of the basic data protection principles, the amount of the fine can go up to 20 000 000 euros, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[70] *Secondly*, according to *Hildebrandt*, the concept of procedural justice in the context of law always requires a decision.[71] As any alleged infringement of the Regulation can be brought up to a supervisory authority, the importance of proof concerning the implementation of the principles is significant.[72] In other words, the

[67] For an international perspective on the basic data protection principles: *Bygrave, Lee Andrew*. Data Privacy Law: An International Perspective, Chapter 5 Core Principles of Data Privacy Law.
[68] Bird & Bird GDPR Guide. 2. Principles. A. Data protection principles.
[69] *Nevasalo and Parviainen* 2017, p. 29.
[70] Article 83(5a) of the Regulation.
[71] *Hildebrandt* 2014, p. 50 – 52.
[72] Article 77 of the Regulation.

effective and recorded implementation of the basic principles provides protection for the app developer in the case of an alleged infringement of the Regulation.

In addition to the basic data protection principles, the general obligation to protect personal information undergoing processing *by design and by default* should be at the very core of the data protection practices within the app. This concept is relevant in the implementation of the principles and creates further safeguards in relation to the end users.[73] According to the concept, technical and organisational data protection measures should be designed in a way which best implements the basic principles. In doing so, the app developer should take account of each specific processing context and choose a design which is proportionate to the implementation costs and to its effects on the end users' rights and freedoms.[74] In addition to the design, the app developer should implement sufficient technical and organisational data protection measures by default. This practice ensures that the basic principles are respected by processing only data which is necessary for each specified processing purpose.[75]

In connection to data protection by design and default, the *accountability principle* (7) obligates the app developer to demonstrate compliance with all other basic principles on a general level. Specifically, accountability means anticipating the dangers that data processing imposes on personal information. In order to comply with the principle, the app developer should clearly allocate data protection responsibilities inside its organisational structure and determine appropriate security measures protecting the acquired data.[76] Moreover, both the app developer and all its data processors are obliged to ensure that their policies, codes of conduct and training programs respect the basic principles. Compliance should be demonstrated objectively, meaning precise documentation covering all processing decisions, and possibly, adoption of a specific data protection impact assessment.[77]

---

[73] Article 25 of the Regulation.
[74] *Klitou* 2014, p. 262.
[75] *Andreansson and others* 2015, p. 9 – 10.
[76] *Aalto-Setälä* 2016. EU:n tietosuoja-asetus tulee – valmistaudu ajoissa. Chamber of Commerce of Finland.
[77] Bird & Bird GDPR Guide. 2. Principles. A. Data protection principles.
Data protection impact assessment is stipulated in Article 35 of the Regulation.

2.2.2.1. Data minimisation and data quality

As addressed above in Sub-Chapter 2.1.1., pets' location data normally connects to supplementary information on the end users or other identifiable individuals. By collecting and combining characteristics associated with a certain location, the app developer can, in theory, deduct information on the individuals' visits to hospitals, political gatherings, and religious events. However, to respect the *data minimisation principle* (1), the app developer should introduce practices which effectively preclude the possibility of excessive data collection. In doing so, the challenge is to keep adequate records which practically verify data minimisation, and to limit ongoing collection of location data.

In the Regulation, the data minimisation principle sets forth that all collected personal information needs to be adequate, relevant, and limited to what is necessary for each specific processing purpose.[78] On the contrary to the unlimited collection and retention of personal information, the principle requires that only strictly necessary data is collected. The benefits of data minimisation include easier organisation, better control, and lower risk of data breaches. In addition, data minimisation is economically effective as managing smaller amounts of data requires less resources than organising masses of unnecessary information.[79]

Technically, it is impossible for the app developer to remove the connection between the location of a pet and end user. Instead, it should sufficiently implement data minimisation by prudently applying the storage limitation and purpose limitation principles as addressed below in Sub-Chapter 2.2.2.2.. According to these principles, location data should be stored only for limited time periods and processed for clearly detailed purposes. These practices ensure that no highly sensitive and accurate profiles connected to natural persons are formed over time. On request, the practices should be objectively verifiable, meaning that the extent of the data processing is demonstrated by precise documentation. In doing so, the collection of strictly necessary personal information and the deletion of any unnecessary or dated data[80] form the foundation of minimal data processing. Moreover, it is easier for the app developer to verify that

[78] Article 5(c) of the Regulation.
[79] *Marr* 2016, p. 1 – 2.
[80] *Aukia* 2018, p. 12.

smaller amounts of information do not include excessive or illegally collected data.

As mentioned above, record-keeping objectively verifies the fulfilment of the data minimisation principle. In addition, record-keeping is a legal obligation found in Article 30 of the Regulation. In this Article, it is stipulated that all relevant processing activities should be adequately recorded. In detail, the records should include descriptions of the processing purposes, categories of the data subjects, as well as categories of the processed personal data.[81] In order to protect smaller data controllers conducting occasional data processing, the obligation does not concern enterprises or organisations employing fewer than 250 persons.[82] However, the exception does not apply if data processing is likely to result in a risk to the rights and freedoms of the data subjects, the processing is not occasional, or the processing includes special categories of personal data (defined later in Sub-Chapter 2.2.3.7.). In the context of the pet monitoring app, the data collection is not occasional and might include special categories of personal data. Therefore, the app developer should keep accurate processing records not only to verify data minimisation, but also to fulfil the legal obligation. In other words, even if the record-keeping obligation of Article 30 would not apply to the app developer, records would still have to be kept for the verification of data minimisation. Subsequently, the rule that smaller entities do not need to keep records of their processing activities can be misleading in relation to the data minimisation and other basic data protection principles.

Furthermore, it is an interesting factor to consider, whether the data minimisation principle allows the app to collect ongoing location information. This kind of collection is possible, among others, by passive scanning within the WiFi infrastructure. By constantly accessing location data transmitted by the electronic collars and the operating mobile devices, the app would always know where the pets, and subsequently, the end users reside. As to the opinion of the writer, different practices should be introduced in relation to the mobile devices and the electronic collars. *Firstly*, a mobile device is an extremely private object closely connected to its owner. Processing its ongoing location for the purposes of pet monitoring would violate the data minimisation principle.

---

[81] Article 30 of the Regulation.
[82] Article 30(5) of the Regulation.
For a detailed definition of '*small enterprise*': Recommendation of the European Commission concerning the definition of micro, small and medium-sized enterprises, C(2003) 1422.

Therefore, the location of the mobile devices should be accessed only when the app is turned on. If sufficient for the smooth operation of the app, processing the data should also be limited to tracking the pets within the GPS infrastructure. *Secondly*, the purposes of the data collection allow the app to process ongoing location data transmitted by the electronic collars. Without this kind of information, the app would not able to form the accurate activity profiles constituting an integral part of its operations. Moreover, the location of the electronic collars is only indirectly connected to the end users, and the rights and freedoms of the individuals do not override the purposes of this kind of data collection.

In connection to data minimisation, the app developer needs to respect the *data quality principle* (2). In this regard, the main obligation is to technically organise the collection of accurate data as opposed to focusing on precise record-keeping. For example, the app developer contributes to data quality by operating the app within the GMS, GPS and WiFi infrastructures, in other words, in the context of a hybrid service. In this way, the combination of the commonly used infrastructures enables the best locating outcome and ensures the accuracy of the location data. In addition, the app developer can work in cooperation with the OS manufacturers to constantly improve the platform of data collection.

In the Regulation, the data quality principle requires that personal data undergoing processing is accurate and that inaccurate information is erased or rectified without delay.[83] Both data minimisation and data quality emphasise better data management which benefits the data controllers and the data subjects. For the data controllers, accurate information makes decision-making easier, increases work productivity, and facilitates targeted marketing. For the data subjects, data quality means correct processing outcomes, compliance with the data protection legislation, and smaller risk of reputational damage resulting from decisions based on inaccurate information.[84] As a concept, the data quality principle does not impose any significant obligation which would not be included in the implementation of data minimisation.

[83] Article 5(d) of the Regulation.
[84] *Moreno* 2017, p. 1.

2.2.2.2. Storage limitation and purpose limitation

The app developer should respect the *storage limitation principle* (3) by limiting the retention of personal information to the strict minimum necessary to monitor the pets. In this regard, the problem is that locating the pets cumulatively for their lifetime would be beneficial to the app developer's processing purposes. However, this kind of data retention is not enough to implement storage limitation. Many pets live somewhere between 10 and 20 years and accumulating information during this entire period would qualify as excessive data retention. Preferably on a monthly or similar basis, the app should delete all personal data that is no longer necessary to form the current activity profiles.

The storage limitation principle is stipulated in Article 5(e) of the Regulation. According to this Article, personal data should be kept in a form which permits identification of the data subjects for no longer than is necessary for the processing purposes. The principle requires that the data subjects know the length of the data storage period, or alternatively, the criteria determining the period. In this regard, the length of the period should reflect the processing purposes.[85] Moreover, storage and deletion of the personal data should be organised in a way which minimises the risk of data breaches.

In addition to risk minimisation, the app developer should ensure that each data processor under its control complies with the storage limitation principle.[86] As already addressed regarding the data minimisation and data quality principles, managing the technical execution is the most demanding obligation also in this context. The app developer should regulate and record its own data storage, but also all storage carried out by relevant third parties. As an example, data storage delegated to a cloud service supplier should be controlled by the app developer. Commonly, this supplier would base its commercial relationships on the standard terms of business not modifiable by individual clients. Therefore, the app developer would have only marginal control over the actual processing and storage operations. Despite the practical difficulty, the legal obligation to control would not be shifted to the data processor.

---

[85] *Fredman* 2017, p. 10.
[86] *Long and Shankar* 2016, p. 16. International Association of Privacy Professionals (IAPP).

Legally, personal data can be collected only for specified, explicit, and legitimate purposes (the *purpose limitation principle* (4)).[87] For the app developer, the original processing purpose is to form the ongoing activity profiles. Without a supplementary legal basis, an additional processing purpose is not compatible. As an example, using the pets' location data to monitor the daily habits and routine movement patterns of the end users would not qualify as a compatible additional purpose.[88] In this case, the inferred data would reveal excessive sensitive information on the end users and considerably increase the extent of the data collection. Therefore, an additional processing purpose is compatible only if it is foreseeable to the end users, and by its nature, does not require further safeguards to be met. Otherwise, another legal basis should be acquired.

Article 6(4) of the Regulation sets the basic criteria for determining the compatibility of the original and additional processing purposes. *Firstly*, before processing data for additional purposes, the existence of any link between the original and additional purposes should be verified. Here, the context within which the personal data was initially collected and the nature of the data influence the legitimacy of supplementary processing. *Secondly*, the possible consequences of further processing and the lack of adequate safeguards may render additional purposes incompatible. Moreover, further limitations apply on a case-by-case basis.[89]

According to *Hildebrandt*, the ethical concept of contextual integrity is an integral part of the legal concept of purpose binding. Contextual integrity means that the extent of the purpose limitation principle depends on the context within which or the contexts between which the data is processed. For example, in the context of a business transaction the scope of legitimate processing is considerably broader than in the context of healthcare. Subsequently, in determining the compatibility of the original and additional processing purposes, the app developer fundamentally faces the challenge of defining the contextually legitimate extent of data processing.[90]

[87] Article 5(b) of the Regulation.
[88] In addition, targeted marketing would not qualify as a compatible additional processing purpose.
[89] Article 6 of the Regulation.
[90] *Hildebrandt* 2014, p. 50 – 57.

2.2.2.3. Data integrity and confidentiality

Technically, the pet monitoring app combines information from two smart objects, the electronic collars and the operating mobile devices. In their research, *Chen and others* have defined this context as the Internet of Things (later referred to as '*the IoT*').[91] By definition, the IoT is "*the concept of pervasive interconnected smart objects operating together to reach common goals*".[92] When collecting, transferring or otherwise processing personal data within this context, the responsible data controller should adopt sufficient and adequate security measures to effectively respect the *data integrity and confidentiality principle* (5). Within the pet monitoring app, the main practical challenge connected to these security measures is to ensure that the used locating techniques are robust. In addition, the app developer should implement appropriate cryptography to protect location data transferred between the electronic collars and the operating mobile devices.

According to Article 5(f) of the Regulation, data integrity and confidentiality fundamentally means that personal data is processed in a way which ensures appropriate security of the data. '*Appropriate security*' includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage, and inappropriate technical or organisational measures.[93] As a shortcoming, the technological level or type of the required security measures is not specified in Article 5(f). The data controllers need to define themselves, which kind of economic and technological resources they are willing to invest. Despite this practical challenge, the implementation of the security measures should start from the design of the databases and electronic platforms.[94]

In order to securely collect and transfer location data within the IoT, the app developer should make sure that the systems used for locating are robust.[95] As an example, a danger to system robustness is the fact that any locating infrastructure might be subject to security vulnerabilities caused by third parties or other external factors. Space weather or system breakdown might affect the locating precision of the GPS infrastructure. Moreover, intentional interference might change or modify locating

[91] *Chen and others* 2017, p. 8964 – 8968.
[92] Ibid., p. 8956.
[93] Article 5(f) of the Regulation.
[94] *Aukia* 2018, p. 11.
[95] Ibid., p. 12.

outcomes in all infrastructures. Some of the vulnerabilities might not be foreseeable to the app developer, but in general, it should assure the highest possible level of system robustness. In this regard, the appropriate measures enhancing robustness include signal quality monitoring and error correction.[96]

In connection to ensuring system robustness, the app developer should use standard cryptography to protect the transfers of location data between the electronic collars and the operating mobile devices. In doing so, cryptography adds another level of protection after the locating technology of the smart objects is verified to be correct up to a certain precision and trusted by the parties to the transfer. A cryptographic technique helps the app developer to preserve the authenticity and integrity of the transferred information by ensuring that the information is sent by the correct source and that it has not changed during the transfer. For example, cryptographic techniques for smart objects include secret- or public-key encryption, message authentication, digital signature, and authenticated encryption.

In addition to data authenticity and integrity, the app developer should choose a cryptographic technique which preserves the confidentiality of the data transfers. According to *Chen and others*, the best available cryptographic solution to cover all three requirements is the secret-key encryption. This technique is based on a secret-key which is shared between the parties to the transfer and which reveals the transferred information. Furthermore, the secret-key encryption ensures that only the intended parties have access to the transferred data and that no third party can affect the integrity of the information. On the down side, the secret-key encryption requires extensive implementation resources. Therefore, it might be too expensive for the app developer with relatively limited funds to use the technique efficiently and securely.

In addition to the secret-key encryption, specific lightweight cryptography has been designed to offer security with lower implementation costs. This kind of cryptography requires smaller circuit footprint, lower power consumption, and lower memory requirements.[97] Unfortunately, the new technology can operate only with specific sensitive hardware that still needs to be developed and researched further before it

[96] *Chen and others* 2017, p. 8958 – 8964.
[97] Ibid., p. 8964 – 8967.

becomes economically and technologically feasible.[98]

Even after the app developer has ensured robustness of the locating systems as well as integrity, authenticity, and confidentiality of the location data, the transferred information might still be endangered. As an example, if location data is transferred within the WiFi infrastructure, the first access nodes connecting an electronic collar to the network know that the device is within the range of a specific access point. As a solution, the app developer can protect the data by using the techniques called anonymisation and pseudonymisation.[99] According to Recital 26 of the Regulation, anonymisation means that personal data is rendered anonymous in a way which no longer allows the identification of an individual. Unlike pseudonymised information, anonymised information does not qualify as personal data.[100] According to Article 4(5), pseudonymisation "*means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". Nevertheless, both techniques can be used to protect location data while the information is transferred over a network. If correctly implemented, anonymisation and pseudonymisation hide all information (including the first access nodes) which would allow the identification of the individuals. In practice, implementing the techniques has proved difficult as tracking an individual might be possible even after the first access node information has been correctly anonymised or pseudonymised.[101]

As an alternative to address the problem of the first access nodes, the app developer can prefer to transfer the personal information within the Bluetooth infrastructure. As mentioned in the introduction to this thesis, the app transmits the location data either within the WiFi or the Bluetooth infrastructure. In this regard, the technology and security vulnerabilities of the WiFi infrastructure were already addressed in Sub-Chapter 2.1.2.. On the other hand, the Bluetooth infrastructure enables smart objects to connect in the unlicensed industrial, scientific, and medical (ISM) frequency band. This

[98] Ibid., p. 8970.
[99] Ibid., p. 8967.
[100] Recital 26 of the Regulation.
Tarhonen 2017, p. 29 – 32.
[101] *Chen and others* 2017, p. 8967.

technology uses multiple radio frequencies to transmit information and ensures the fastest connection over multiple radio channels with the Adaptive Frequency Hopping Technology. The specific Bluetooth technique used within the app is called Point-to-Point, offering a device communication between two smart objects.[102] Due to the recent development, the Bluetooth infrastructure has significantly increased its range and speed of transmission. However, like the WiFi infrastructure, also the Bluetooth radio transmissions are sensitive to security vulnerabilities caused by third parties and other external factors.[103] Therefore, the sole existence of the first access nodes does not render the Wifi infrastructure more security vulnerable. Both transmission contexts need to be adequately protected with sufficient cryptography. Therefore, the combination of the two techniques is a way to increase data transmission possibilities, not to enhance data security.

In conclusion, there is currently no perfectly feasible method to fully preserve integrity and confidentiality of location data collected and transferred within the app. The app developer should use standard cryptography and other techniques which adequately protect the rights and freedoms of the individuals. Sufficiency of the security measures should be demonstrated by precise documentation and adjusted according to the technological development in the future.[104]

2.2.2.4. Fairness and lawfulness

In relation to the end users, the most noteworthy data protection obligation of the app developer is to collect location data fairly, lawfully, and transparently. In the Regulation, this obligation is included in the implementation of the *fairness and lawfulness principle* (6). The principle is defined in Article 6(1) and sets forth that data processing is lawful *only if and to the extent that* at least one of six specific requirements applies. The requirements are:

- *Data subject has given consent to the processing;*
- *Processing is necessary for the performance of a contract to which the data subject is*

[102] Bluetooth Technology -website. Radio Versions.
[103] *Kelley* 2016. Is Bluetooth Security Good Enough for Your Most Sensitive Corporate Communications? Security Intelligence.
[104] *Aukia* 2018, p. 11.
According to *Koski* (2017, p. 61) it will be important in the future to develop new ways to enhance data protection within the IoT so that the focus of the data protection shifts from the data collection limitations and consent requirement to limiting the actual processing and usage of personal data.

party or in order to take steps at the request of the data subject prior to entering into a contract;

- *Processing is necessary for compliance with a legal obligation to which the controller is subject;*
- *Processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
- *Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or*
- *Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

The fact that consent is mentioned in the list as the first requirement does not signify priority over the five other requirements. This approach was recognised in the preparatory works of the Directive and has been applicable ever since.[105] In practice, consent has been the most used legal basis for data processing, and subsequently, it has been addressed in various legal literature. For the pet monitoring app, consent is the main way to legalise the collection of location data and is addressed later in Sub-Chapter 2.2.3.. Performance of a contract and processing in a legitimate interest are further requirements possibly actualising in the context of the app. Therefore, they are summarily addressed below.

Performing a contract to which a data subject is party applies to limited situations, such as to acquiring an individual's home address to deliver goods purchased online, or to obtaining credit card details to effectuate a specific payment. In addition, the contract performance requirement applies to taking steps at the request of a data subject prior to entering to a contract. As an example, responding product enquiries might require processing a person's name and contact details.[106] In the context of the information society services, transmitting communications normally qualifies as contract performance. In this regard, a data subject's username or e-mail address may be disclosed to the parties to the communication without additional legal basis.[107] For the pet monitoring app, transmitting communications is not an original processing purpose. Therefore, the contract performance requirement has a rather limited applicability within the app and is primarily left outside the scope of this thesis.

[105] *Kosta* 2013, p. 231 – 232.
[106] *Gabel and Hickman* 2017. Chapter 7: Lawful basis for processing – Unlocking the EU General Data Protection Regulation. White & Case LLP.
[107] Opinion 02/2013 of the Working Party, p. 16.

The legitimate interest requirement applies to the operations of private entities. To rely on the requirement, the legitimate interest of a data controller needs to be in balance with the rights and freedoms of the data subjects.[108] In other words, the reasonable expectations of the data subjects need to be acknowledged when applying the requirement. In practice, an already existing relationship between a data controller and data subject supports the formation of a legitimate interest. As an example, personal data may be processed in a legitimate interest for direct marketing purposes after the establishment of a commercial relationship between a marketer and client. Furthermore, as stipulated in Recitals 48 and 49 of the Regulation, the concept of legitimate interest includes transmitting personal data within a group of undertakings for internal administrative purposes. It might also include data processing to the extent strictly necessary and proportionate to ensure network and information security. Organisationally, reliance on a legitimate interest requires that the responsible data controller keeps records of the protective measures for the data subjects' rights and freedoms and of the legitimacy of its own interest. The record-keeping demonstrates that the expectations of the data subjects are adequately respected.[109] In the context of the pet monitoring app, processing in a legitimate interest is relevant only to some extent and rather marginal in comparison to the consent requirement.

2.2.3. Consent of data subject

2.2.3.1. General

As defined above, consent is the main way for the app developer to legalise the collection of pets' location data in relation to the end users. In this regard, both the Regulation and the ePrivacy Directive contain provisions regulating the concept. In the Regulation, consent is one of the six requirements rendering data processing lawful. In the ePrivacy Directive, consent is required for storing information or gaining access to information already stored on the terminal equipment of a subscriber or user. In order to distinguish legal obligations, the difference between the two consent requirements is significant. In practice, the requirements might be fulfilled by combining them into one singular consent without affecting the separation of the legal obligations.[110]

---

[108] Recital 47 of the Regulation.
[109] Bird & Bird GDPR Guide. 2. Principles. A. Data protection principles.
[110] Opinion 02/2013 of the Working Party, p. 14.

Both consent requirements are subject to the definition of the Regulation, found in Article 4(11):

> "*Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

This Chapter focuses on the five factors constituting a valid consent, being freely given, specific, informed, indication of wishes, and unambiguous. In order to lawfully collect location data, the app developer needs to effectively respect each factor. In practice, implementing all factors requires management of numerous practical difficulties which are separately addressed in the following Sub-Chapters.

2.2.3.2. Freely given

The first requirement for valid consent is that the consent must be *freely given*. A freely given consent is an act of informational self-determination and is provided without external manipulation. The app developer needs to ensure that the consents acquired from the end users are provided by a clear affirmative action and that they practically leave a real choice for these data subjects. An ambiguous or obscure indication does not suffice to fulfil the criteria.

In legal literature, the absolute starting point for the definition of '*freely given*' has been the difference between voluntary and involuntary actions. *Beyleveld* and *Brownsword*[111] have concluded that the distinction between completely involuntary actions in the strict sense and voluntary actions under pressure is the factor determining whether an action is freely made. If a consent is given due to a negative act of force (*e.g.* duress), it generally is not valid. However, if a consent is given under positive pressure (*e.g.* inducements, discounts, premiums), it does not *in itself* invalidate the given consent.[112]

In the context of the pet monitoring app, no negative acts of force normally affect the acquisition of the end users' consents. Upon free will, each end user has the possibility to download the app from an app store. Only in a very extreme case, a negative act of force could affect an end user such as if the OS of a mobile device would *require* the

[111] *Beyleveld and Brownsword* 2007, p. 141.
[112] *Kosta* 2013, p. 169 – 176.

end user to make use of the app. In doing so, the app would leave no real choice for the end user to determine the benefits of the app usage. On the other hand, positive acts of force are a very common mean for the app developer to enhance the app usage. For example, the app developer might want to offer in-app purchases for a lower price to induce the end users to make further purchases. As mentioned above, the positive acts of force do not *per se* render a given consent invalid. Nevertheless, the app developer should ensure that the offered inducements do not mislead the end users. In these cases, consent is freely given only if the amount of the positive pressure does not result into a negative act of force.

In order to qualify as a clear affirmative action in the meaning of the Regulation and the ePrivacy Directive, a consent should satisfy the consent requirements found in both legal instruments. For the fulfilment of the consent requirement of the ePrivacy Directive, a consent should be acquired before or while the app is installed on a mobile device. In doing so, the consent is acquired before storing information or gaining access to information already stored on the terminal equipment. However, this kind of consenting does not necessarily suffice to fulfil the consent requirement of the Regulation. A consent to the actual processing of personal data should be acquired before an end user starts to use the app after having installed the app on the terminal equipment. As mentioned above, the two consent requirements can be fulfilled by combining them into one singular consent. However, if the combination leads to ambiguity, other requirements for valid consent might not be fulfilled. Therefore, combination should be avoided and implemented only if it contributes to better communication between the app developer and the end users.

Furthermore, the practical implications of freely given have been addressed in various contexts. For example, the Working Party has concluded concerning health records that "*any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free'*".[113] On the other hand, consent cannot be considered freely given if a legal or factual dependency limits the choice of a data subject. This kind of reliance on consent could appear in the relationship of an employer and employee, or if a data subject is in economic duress.[114] In the case of the app, the app developer normally has better understanding on the technological aspects relating to

[113] Working Document 00323/97/EN of the Working Party, p. 8.
[114] *Kosta* 2013, p. 169 – 202.

the data collection and better economic resources than the end users. Therefore, in the case of obscurity or ambiguity, the concept of freely given should be interpreted in favour of an end user. This conclusion does not mean that the relationship of the app developer and end user is assimilated with the relationship of an employer and employee (or a doctor and patient), but that it has similar characteristics regarding the imbalance of knowledge and power.

Another interesting factor concerning freely given is the debate between opt-in and opt-out consents[115]. '*An opt-in consent*' is a valid, freely given indication of a data subject's wishes. According to *Kosta*, opt-in means consent expressed in any affirmative action, such as signing a document, ticking a box, or swiping on a screen, allowing the processing of personal data for a specific purpose. Prior to the adoption of the Regulation, the Working Party had called for clarification regarding the confusion surrounding opt-in and opt-out consents. It had notified that strengthening the data subjects' position requires consents to be given in an explicit, opt-in form.[116] Accordingly, the Working Party had recommended in 2011 (concerning response to letters) that if an individual has not taken any positive action to provide consent, the lack of behaviour should not be interpreted as consenting. Regarding direct marketing emails, the Working Party had further specified that pre-ticket boxes on websites are not compatible with the definition of consent under the Directive.[117] As a matter of fact, '*an opt-out consent*' is a mere expression of a data subject's right to object.[118] Specifically, opt-out means failure to take an action, such as leaving a box unticket, resulting in the assumption of consenting, unless ticket.[119] Within the app, opt-in means that the end users have a real possibility to make a choice. By clicking *install or accept* they consent to the storing, gaining access, or actual data processing.[120]

[115] Ibid., p. 188 – 189.
[116] The Future of Privacy – Joint contribution 02356/09/EN of the Working Party, p. 8.
[117] Opinion 15/2011 of the Working Party, p. 24.
[118] *Kosta* 2013, p. 199 – 200.
According to Article 21 of the Regulation, the data subjects have the right to object to data processing resulting in profiling based on automated decision-making, or to data processing for direct marketing purposes.
[119] *Kosta* 2013, p. 188 – 189.
[120] Opinion 02/2013 of the Working Party, p. 14.

2.2.3.3. Specific

The second requirement for valid consent is that the consent must be *specific*. The app should respect the specificity requirement by providing necessary processing information to the end users. In this regard, the end users should be notified that the app accesses limited data categories transmitted by the electronic collars and by the operating mobile devices. Regarding location data in general, the end users should be informed on the accuracy of the locating techniques. In doing so, the end users provide specific consents without any lack in transparency affecting their free will.[121] Within the app, the main difficulty associated with the implementation of the specificity requirement is to objectively verify that only specified categories of personal data are collected (*consent demonstration*).

In the Regulation, the specificity requirement is clearly linked to the informational requirement. As a rule, consent is specified by information provided to the data subjects. Specificity means that all collected personal data and conditions surrounding the data processing are clearly detailed.[122] The degree of specificity depends on the type of data processing and increases with the impact it has on the data subjects' rights and freedoms. Moreover, the data subjects should be reminded on the data processing on a yearly or similar appropriate basis.[123]

In legal praxis, the specificity requirement has been elaborated in multiple contexts, such as in the Opinion of the Advocate General *Sharpston* in joined cases *Volker und Markus Schecke GbR/Hartmut Eifert v Land Hessen*[124] of the Court. In the Opinion, the Advocate General addressed the problem of specifying a signed statement in an application form for agricultural subsidies. In the case, the form did not make unambiguously clear, and therefore, was not specific enough, that the applicants had consented to the online publication of name, municipality of residence, and awarded amounts. Substantially, the case demonstrated a need to find balance between two different fundamental principles, the transparency of subsidising and the data subjects'

[121] Ibid., p. 6.
[122] Recital 39 of the Regulation.
[123] Opinion 13/2011 of the Working Party, p. 15 – 16.
[124] Joined cases C-92/09 and C-93/09 of the Court.

right to data protection. In this regard, it should had been ascertained that the data subjects were informed on all effects the processing had on their fundamental rights.[125]

Like in the Opinion, also in the context of pet monitoring the extent of specificity is determined by the fundamental principles affecting the data processing. Within the app, location data is collected to provide the geolocation services to the end users and to contribute to the business operations of the app developer. In this regard, the fundamental conflicting principles are the app developer's economic liberty and the data subjects' right to data protection. As a rule, purely economic values should not override the fundamental rights and freedoms of individuals. Therefore, the app developer is responsible for ascertaining that all data subjects are sufficiently informed on the effects the data processing has on their personal information. Moreover, the information notices should be more detailed than, for example, in the case of providing information between two enterprises.

In practice, efficient implementation of the specificity requirement has proved extremely difficult as demonstrated by recent claims on *Facebook* regarding the listening of daily conversations through mobile devices' microphones. In order to provide targeted marketing, the multinational enterprise had used the latest techniques to combine data from multiple sources. Despite the statements in its privacy policy, the extreme relevancy of the displayed advertisements had caused vast public concern regarding the illegal use of the microphones. The claims argued that Facebook had acquired excessive personal data for the sole purpose of targeted marketing.[126]

The *Facebook* case demonstrates how difficult it is to verify that only specified categories of personal data are collected and that all other data processing is effectively excluded. This difficulty is relevant also in the context of the app and needs to be taken account of in the design and development of its privacy statements. Officially, the data subjects are granted the right to subject access in Article 15 of the Regulation.[127] On request, the app developer is obliged to confirm whether an individual's personal data is

[125] Opinion of Advocate General Sharpston in joined cases C-92/09 and C-93/09P of the Court, p. 11093.
[126] *Titcomb* 2017. 'Facebook is listening to me': Why this conspiracy theory refuses to die. The Telegraph.
[127] The right to subject access reflects the right to informational self-determination, meaning that an individual has the capacity to independently determine first whether his or her personal data is disclosed, and subsequently, how it is used (Korff 2010, p. 2).

processed, and subsequently, provide access to the data. As a concept, the right is closely connected to the specificity requirement and gives the end users the possibility to effectively verify the extent of specific data processing. In this regard, the Working Party has recommended that in order to verify a specific consent and its extent, a data controller operating in the online environment should retain information on the session in which the consent was expressed. In addition, it should record the documentation of the consent workflow and a copy of the information that was presented to the data subject. In doing so, the app developer respects the requirement of consent demonstration and ensures that specific details relating to the consent acquisition are verifiable in the future.[128]

Another important factor connected to the specificity requirement is the purpose limitation principle. Traditionally, there has been no common understanding whether the specificity requirement allows data processing for multiple purposes.[129] Currently, in Recital 32 of the Regulation, it is stipulated that if data processing has multiple purposes, consent needs to be given for all of them. Instead of setting an absolute number of purposes, the data protection framework limits the way the app developer communicates the processing purposes to the end users. The correct communication means that the end users understand the meaning of each processing purpose and provide separate opt-in for all of them.[130] Furthermore, no excessive purposes resulting in confusion or ambiguity should be communicated. As an example, an excessive processing purpose would be *market research* without any further specification.[131]

2.2.3.4. Informed

To acquire an *informed* consent, a data controller needs to provide sufficient and appropriate information to the data subjects regarding fundamental aspects of intended data processing. The categories of relevant information are set forth in Articles 13 and 14 of the Regulation. In the context of the pet monitoring app, the app developer should provide information in a granular structure which best serves the end users. Each layer of the structure should include only the adequate facts connected to the collection of

[128] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 20.
[129] *Kosta* 2013, p. 219 – 226.
[130] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 13.
[131] Opinion 02/2013 of the Working Party, p. 6.

location data. Essentially, the app developer should avoid *over-valuing* consent by providing excessive information. Moreover, information should be provided in a contextually intelligible form and presented in a distinct page with a clear opt-in feature.

In Articles 13 and 14 of the Regulation, the required information categories vary based on whether personal data is collected from a data subject or whether it is obtained from someone else. Both categories include, among others, identity and contact details of the data controller, recipients of the personal data, as well as original processing purposes.[132] The provided information should be accessible in an intelligible form, which taking account of the needs of the targeted audience[133] in the online environment is presupposed to mean in English.[134] The information should not be excessive, as a fully specific consent is not required to fulfil the informational requirement.[135] According to Articles 13 and 14, the data controllers are responsible to provide the information. Irrespective of the method or form used, the information should be provided at the time personal data is obtained or accessed on terminal equipment.[136]

The Working Party has recommended that the information notices in relation to specific data processing are provided in the layered, granular structure based on accuracy. The recommendation corresponds the concept of extended information as introduced by *Manson and O'Neill* in the field of bioethics. According to the concept, the best way to provide the notices is to give a limited amount of accurate and relevant information, and to offer a user-friendly way to extend the provided amount.[137] The Working Party has recommended that the relevant information is divided to maximum 3 layers.[138] In this regard, a data controller should design the notices in a way which minimises the risk of not reading them.[139] However, after having provided the information in the layered form, the data controller concerned has no fundamental obligation to make sure that the data subjects actually read the notices. Sufficient fulfilment of the requirement ensures that, in principle, the data subjects carry the risk of not comprehending important aspects of the data processing.

---

[132] *Kosta* 2013, p. 204 – 210.
[133] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 14 – 15.
[134] *Kosta* 2013, p. 218.
[135] Ibid., p. 210 – 211.
[136] Ibid., p. 212.
[137] *Manson and O'Neill* 2007, p. 6.
[138] Opinion 10/2004 of the Working Party, p. 8.
[139] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 17.

As recommended by the Working Party, the app developer should use layered information notices both when the app is downloaded to a mobile device, and before the app is taken into use. The first layer should include all fundamental facts relating to the data collection such as the categories of collected personal data, purpose(s) of the processing, and identity of the data controller. In addition, the first layer should contain a clear link to the second, more detailed layer. The second layer should include all recipients of the data, information on whether the data is transferred to third countries[140], information on the data subjects' rights and freedoms, as well as information on how the data controller protects the personal information and keeps records of its processing activities.

In the online environment, information is commonly provided in long and detailed privacy policies[141]. In general, these documents include excessive information not necessary to provide an informed consent.[142] In his research, *Browsword* has addressed this problem of vast information notices. By presenting excessive information to the data subjects, the data controllers over-value the concept of consent. '*Over-valuation'* means that consent is considered the sole sufficient basis to protect the fundamental rights and freedoms of the data subjects while rendering data processing lawful.[143] In principle, the data subjects carry the risk of not paying necessary attention to the provided information before consenting. However, in the case of no or marginal direct communication between a data controller and data subject (as common in the online environment), the data subject's rights and freedoms should be further protected by the data controller.[144] This protection is necessary to reinforce the data subject's weaker bargaining position and lack of knowledge.[145] In the context of the app, a privacy policy can be included in the information structure. In doing so, it can be used as the second or even as the third layer. However, the privacy policy should be accurate in a way which best fulfils the informational requirement. If the privacy policy lacks accuracy, the app developer carries the risk of not acquiring an informed consent.

---

[140] The European Commission's website. A country outside the EEA. Adequacy decisions.
[141] According to Business Dictionary, '*privacy policy*' is a statement which declares a firm's or website's policy on collecting and releasing information about a visitor. It usually declares what specific information is collected and whether it is kept confidential or shared with other firms, researchers, or sellers.
[142] *Kosta* 2013, p. 215 – 218.
[143] *Brownsword* 2004, p. 224.
[144] *Beyleveld and Brownsword* 2007, p. 154.
[145] *Bräutigam* 2012, p. 426.

2.2.3.5. Indication of wishes

Consent is an *indication of wishes* and signifies agreement to the processing of an individual's personal data. Within the pet monitoring app, consents are primarily acquired in an electronic form. This kind of affirmative action, such as clicking a box, is verifiable in the future if records are kept of the terminal equipment which have accepted the data processing. In doing so, the real challenge connected to the wish indication requirement is to determine *who* has consented to the collection of location data. Without any further identification, an electronic consent verifies that *someone* has provided acceptance. It does not identify an end user, ascertain that the end user is not a child, or include any verifiable way to acquire the consent of a holder of parental responsibility. In addition, the app is not able to distinguish, how a pet's location connects to the location of multiple individuals. A pet can reside close to an end user, but also close to the end user's family and friends, neighbours, or even strangers. Therefore, the app would often collect location data connected to individuals who have not indicated their wishes to disclose personal information.

Prior to the adoption of the Regulation, debate was conducted on the consent of minor.[146] According to *Kosta*, physical or legal incapacity prevents a data subject from providing valid consent. In these cases of incapacity, only a statutory or legal representative can indicate the wishes of the data subject.[147] Currently, it is set forth in Article 8 of the Regulation that if an information society service is offered to a child, the child is able to give his or her consent to the processing if being at least 16 years old. Otherwise, the consent should be provided or authorised by a holder of parental responsibility over the child. In addition, the Member States may determine lower age limits while the absolute minimum is 13. In these cases, the validity of the consent depends on the practices of the Member State concerned and should be determined based on a child's maturity level or similar objective factors.[148]

In the online environment, it has been the general practice to verify the age of the Internet users by asking how old they are.[149] However, in the era of the current data

[146] *Kosta* 2013, p. 159 – 161.
[147] Ibid.
[148] Ibid., p. 160 – 165.
[149] *Bräutigam* 2012, p. 423 – 425.

protection framework, it has become questionable whether this kind of affirmation fulfils the wish indication requirement. According to *Bräutigam*, the best available identification of an end user is verification with the credit card details. The credit card details verify that an end user personally accepts the data processing and that he or she is not a child. In a similar way, the credit card details can be used to acquire the consent of a holder of parental responsibility over a child. On the down side, this kind of identification leads to further data processing and raises questions of necessity.[150] Additionally, there is currently no centralised system in the EU to combine information of a child and a holder of parental responsibility.[151] As an alternative, many mobile devices offer access control and identification with the fingerprint technology.[152] This technology is noteworthy, as it can verify that same person downloads the app to a mobile device and later accepts the collection of personal data. For the control of a person's age, the technology offers only the information that the end user concerned has provided to the OS offering the identification system.

Regarding age verification, the Working Party has notified that verifying the data subjects' ages requires reasonable efforts from the responsible data controller. *In low risk situations*, like in the context of an online gaming platform, the data subjects can be asked how old they are. If a data subject states that he or she is under the age which allows the lawful indication of wishes, the consent of the holder of parental responsibility can be acquired by sending an email or similarly asking for acceptance. Furthermore, the responsible data controller needs to make reasonable effort to verify that the sender of the response email or the provider of acceptance actually holds the parental responsibility. In the case of a complaint, further age verification is required. *In high risk situations*, age verification may be acquired by using trusted third party solutions. These solutions should not lead to excessive data processing, and therefore, identification with the credit card details does not satisfy the requirement. The data controllers should follow the technological development and implement the best available technique.[153]

[150] Ibid.
[151] *Aukia* 2018, p. 13.
[152] *Blanchette* 2012, p. 69 – 70.
[153] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 25 – 29.

Collecting pets' location data does not easily fit either one of the categories allocated above. It has characteristics from both high risk (data connections) and low risk (processing purposes) situations. The best available way to verify an end user's age is identification with the credit card details. However, as stated above, this kind of practice leads to significant further data processing and does not fulfil the wish indication requirement. Furthermore, the fingerprint technology is too vague as it leaves the real control over the age verification on the controlling OS. In addition, processing biometric data (fingerprint) leads to supplementary data collection.[154] Due to the impracticalities associated with both techniques, the future practices will have to clarify the form and extent of required identification and age verification. For now, the app developer can legally base its age verification system on asking the end users how old they are and on correctly implementing an email verification system in relation to the consents of holders of parental responsibility.

If a data subject can legally indicate his or her wishes, the wish indication requirement requires two further criteria to be met. *Firstly*, as concluded above regarding the concept of freely given, opt-out does not constitute a valid consent. Some active affirmation is required, presented either in written, oral, or electronic form. *Secondly*, mere silence does not signify consenting. Only some kind of affirmative acceptance may constitute an implied consent qualifying as an indication of wishes. The Court has concluded in joined cases *Zino Davidoff SA v A & G Imports Ltd and Levi Strauss & Co. v Tesco Stores Ltd* that the facts and circumstances which unequivocally demonstrate the intention of a data subject constitute a valid implied consent.[155] Therefore, the app developer should make sure that the end users have a real possibility to refuse the data collection. Having the possibility, the data subjects indicate their wishes on whether using the app and accepting the data processing are worth taking the risks associated with the collection.

In locating, it is unavoidable that a specific location connects to multiple individuals. As argued above, a pet's location connects to the location of an end user, but also to the location of individuals who have not indicated their wishes to disclose the personal data (the end users' family and friends, neighbours, and strangers). In the strict sense, the Regulation would require that each individual whose personal data is collected, *directly*

[154] *Blanchette* 2012, p. 69 – 70.
[155] Joined cases C-414/99, C-415/99 and C-416/99 of the Court, p. 8751.

or indirectly, consents to the data processing or that another legal basis renders the processing lawful. This kind of interpretation would make the development of any location based service extremely infeasible. In practice, it would not be reasonable or even technologically possible to acquire consents from every individual whose location data might be indirectly accessed. Instead, the problem of location data connections can be adequately addressed by respecting the basic data protection principles as presented below.

The core value of the data protection framework is that every individual's personal data is protected. In addition, as stipulated in Recital 2 of the Regulation, the data protection framework is intended to contribute to the economic and social progress of the EU.[156] In other words, the Regulation should not hinder economic activity, but rather enhance data protection inside the internal market.[157] The basic data protection principles are the foundation of the Regulation. Where possible, the principles should be fully implemented to the data processing operations of a data controller. However, as demonstrated in the context of the data integrity and confidentiality principle, it is not possible to ensure full robustness of a locating system or to fully protect personal data from third party data breaches.[158] There are always new harmful technologies not foreseeable to a data controller.

The above statement means that also in the context of the fairness and lawfulness principle the wish indication requirement should be respected to the technologically and organisationally reasonable extent. In doing so, the consent of an end user should be clearly detailed and include information on the indirect location data connections. Moreover, the data minimisation and storage limitation principles should be implemented in a way which precludes the possibility of excessive data collection. No profiling[159] of individuals residing close to a pet should be possible, and targeted marketing based on an individual's specific location should not be introduced. This practice allows the app developer to legally rely only on the consents of the end users.

---

[156] Recitals 1 and 2 of the Regulation.
[157] Communication COM(2017) 9 final of the European Commission, p. 3.
[158] *Aukia* 2018, p. 12.
[159] According to Article 4(4) of the Regulation, "*profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

However, disregarding the above specified obligations is at the very core of the data protection framework and subject to the highest scale of administrative fines.

2.2.3.6. Unambiguous

In Article 7 of the Directive, *unambiguity* was a factor rendering consent, and subsequently, data processing legitimate. In the Regulation, unambiguity is included in the definition of consent (Article 4(11)), meaning that there should be no doubt about the fact that a consent has been given. In this regard, it is important for the app developer to determine how long a given consent remains valid and whether an end user can withdraw a provided indication of wishes.

According to *Kosta*, limited legal debate has been conducted on unambiguity. Some Member States, like Germany and the United Kingdom, had left the requirement out of their national legislation implementing the Directive. As a matter of fact, unambiguity does not offer any real additional value to a valid consent as defined above. In any case, it does not signify that a valid consent could be ambiguous.[160]

Without a doubt, a consent provided for an indefinite time period would be ambiguous and leave excessive control for the data controller. However, the data protection framework does not set any specific, universal time limit defining the temporal extent of a given consent. According to the Working Party, a valid consent should be renewed at appropriate intervals determined by the context of data processing, scope of the original consent, and expectations of the data subject.[161] Accordingly, consents acquired within the app should be renewed on a yearly or similar appropriate basis. In addition, the consents should be refreshed if the app has not been used for a certain time period. Regarding the consents acquired before the application of the Regulation, the app developer should review their compatibility with the new requirements, and possibly, consider renewal.[162]

In addition to the renewal of consent, the data subjects have the right to withdraw a given consent at any time. This characteristic is not included in the definition of

[160] *Kosta* 2013, p. 232 – 234.
[161] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 20.
[162] Recital 171 of the Regulation.

consent, but is an integral part of the legal concept. The right to withdrawal is not dispositive and cannot be waived in relation to the future. This factor distinguishes a consent from the legal concept of contract. Moreover, consent withdrawal does not have any retrospective effect which would affect the legality of prior data processing. Subject to withdrawal, the app developer has no obligation to delete traces of previous processing.[163] Withdrawing should be as easy as consenting and possible at least by the same method used to provide the consent.[164]

2.2.3.7. Special categories of personal data

The pet monitoring purpose does not allow the app to collect health data or similar sensitive information on the end users. Therefore, the app should not directly access any data included in the *special categories of personal data* defined in Article 9 of the Regulation. However, a specific location is automatically connected to further information. Among others, a specific location can be inside a hospital or in front of a church. Subsequently, there is always the possibility that a pet's location reveals sensitive personal information on an end user or another individual. If the app developer disregards this possibility, it might process information included in the special categories without a valid, lawful basis.[165]

In the Regulation, the special categories of personal data are afforded stronger protection as these categories are capable by their nature of infringing the fundamental rights and freedoms of individuals.[166] The special categories are racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, health data, as well as data on individuals' sex life or sexual orientation.[167] Moreover, the categories include genetic and biometric data processed for the purposes of uniquely identifying individuals.[168] The Member States are authorised to introduce further categories that require similar stronger protection.

---

[163] *Kosta* 2013, p. 251 – 254.
[164] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 21 – 22.
[165] Opinion 13/2011 of the Working Party, p. 7.
[166] *Carey* 2015, p. 101.
[167] Article 9 of the Regulation.
[168] According to Articles 4(13) and 4(14) of the Regulation, "*genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*." On the other hand, "*biometric data means personal data resulting from specific technical processing relating to the physical, physiological or*

In principle, any processing of data included in the special categories is prohibited, unless one of the exemptions in Article 9 applies. In comparison to the requirements of lawful data processing as stipulated in Article 6(1), the exemptions are more specific and more compelling. As relevant in the context of this thesis, the first exemption concerns situations where a data subject has given his or her *explicit* consent. According to the early preparatory works of the Directive, the word explicit does not signify an obligation to acquire consent in written form. Instead, it means that the consent must be *absolutely clear*. An implied indication of wishes does not suffice to fulfil the criteria.[169]

Prior to the adoption of the Regulation, the Member States had introduced different interpretations of explicit. Despite the early preparatory works of the Directive, some Member State had adopted legislation which qualified only a written consent as explicitly given. On the contrary, some Member States had set forth that an oral consent can be an explicit indication of wishes. In any case, an explicit consent should be distinctly stated and confirmed with appropriate proof.[170] The purpose(s) of the data processing should be particularly specified and there should be no reasonable doubt about the data subject's free will. Moreover, the EU or the Member State law may further provide that the prohibition to process the special categories may not be lifted by a data subject.[171]

Generally, the app developer is not able to eliminate the potential connection between the collected location data and sensitive personal information relating to identifiable individuals. Instead, it should once again focus on limiting the data collection to the strict minimum necessary to fulfil the purpose of pet monitoring.[172] This limitation means recording the kilometres that pets walk during a day, but not supplementary data connected to these specific movement patterns. The app should not register how often the pets are in specific buildings or places, or find out which functions the buildings or places have.

---

behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

[169] *Kosta* 2013, p. 241 – 251.

[170] Ibid.

[171] Other exemptions for the processing of special categories of personal data are listed in Article 9(2) b-j of the Regulation.

[172] According to *Fredman* 2017 (p. 9), the data processing practices should be adjusted in relation to the risks that the processing imposes on the data subject's rights and freedoms.

Particularly, the data connections impose an obligation to acquire explicit consents in applicable parts. The possibility does not signify that the consents cannot be acquired in an electronic form, but that the information notices are extremely well-organised and specified. If feasible, the app developer should introduce a two-stage consent verification system, using an email link and a subsequent verification code.[173] If the app developer is not able to demonstrate that no data processing is based on the inferred special categories of personal data, it carries the risk of infringing another fundamental component of the data protection framework.

2.3. Synopsys

The first part of this thesis explained, why pets' location data qualifies as personal data, how this information is technically accessed, and which legal instruments regulate the use of this data. In addition, the basic data protection principles and the consent requirement were addressed to elaborate how the data subjects' rights and freedoms should be respected in the context of pet monitoring. The main findings of the first part are allocated in seven arguments. Each argument represents a challenge to the implementation of the app. Three of the arguments concern the basic data protection principles and four of them concern the consent requirement.

Firstly, the data minimisation principle should be at the very core of the app developer's data processing practices. The principle prohibits the collection of personal data connected to the pets' daily movement patterns. If this kind of data would be processed, very sensitive information on individuals' routine habits would be revealed. Furthermore, data minimisation should be respected by directly collecting ongoing location data transmitted only by the electronic collars. Ongoing information transmitted by the operating mobile devices should be accessed only if strictly necessary, such as in the case of finding a missing pet using the GPS infrastructure. The main difficulty in implementing data minimisation is to keep records which demonstrate that the principle is practically respected. In this regard, appropriate records point out the extent of the data collection. Each data subject should also be offered the possibility to access the data, and subsequently, individually verify its minimisation. In general, the Regulation does not set any unequivocal standards on the required record-keeping.

[173] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 18 – 19.

Secondly, the storage limitation and purpose limitation principles regulate the lawful length of data storage and the appropriate purposes of data processing. For the pet monitoring app, it would be profitable to store the collected location data for the life time of the pets. However, in doing so, the app would violate the storage limitation principle. As an alternative, the app should delete collected data on appropriate intervals and make sure that every data processor under its control also respects this obligation. In practice, it might be difficult to track information in the possession of third party data processors, such as information transferred to a cloud service supplier. On the other hand, the purpose limitation principle requires that the end users provide consent to each specific processing purpose and that the purposes are adequately communicated to these data subjects. The Regulation does not set any numeric purpose limitation. In general, the amount of the purposes should not lead to confusion or ambiguity.

Thirdly, the data integrity and confidentiality principle is a new concept in the data protection framework. According to the principle, the app developer should ensure that the locating techniques used are robust and implement standard cryptography to protect the information transferred between the electronic collars and the operating mobile devices. Regarding system robustness, the app developer has only limited possibilities to control the third parties operating the infrastructures. Nevertheless, measures improving system robustness could include signal quality monitoring and error correction. In order to preserve integrity and confidentiality of the data transfers, the app developer should use secret-key encryption or similar standard cryptography to protect the transferred information. If new lightweight encryption is found feasible, it can be used instead of the standard cryptography. In addition, anonymisation or pseudonymisation can be implemented to hide information on the first access nodes. In conclusion, there is currently no existing technology which would ensure full integrity and confidentiality of the collected and transferred location data. The app developer should follow the future development and adjust its practices to the highest available standards.

Fourthly, the app developer should solve the problem of consent demonstration in relation to the end users. The app developer should introduce practices which allow an end user to access his or her personal data without revealing information on other individuals. In this context, the Working Party has recommended that a data controller operating in the online environment verifies a given consent by retaining information on

the session in which the consent was expressed. In addition, it should record the original consent workflow and a copy of the information that was presented to the specific data subject.

Fifthly, over-valuing consent means regarding the data subject's affirmative action the sole sufficient basis to protect his or her fundamental rights and freedoms. In the data protection framework, the consent acquisition is only one factor in comprehensive data protection. It should be respected as any other obligation laid down in the Regulation. The consent acquisition should not signify overriding other basic data protection concepts, such as data minimisation.

Sixthly, consent is an indication of a data subject's wishes. A statutory or legal representative should give his or her approval if a data subject is not able to provide valid consent due to physical or legal incapacity. Consent of a child should be approved by the holder of parental responsibility over the child. For the purposes of verifying the data subjects' age, the data controllers need to introduce different practices in high risk and low risk situations. Regarding the pet monitoring app, asking the end users how old they are currently fulfils the requirement. If an end user indicates that he or she is under the legal age of consent, approval of the holder of parental responsibility can be acquired by an email verification system. Verification with the credit card details would lead to excessive further data processing.

In addition to the problem of age verification, the app developer should address the problem of data connections. Generally, a specific location is always connected to one or multiple individuals. Despite the possibility, the data protection framework does not require that the consents of all these individuals are acquired. Instead, the app developer should correctly implement the data minimisation, purpose limitation, and storage limitation principles to adequately protect the fundamental rights and freedoms of the individuals.

Seventhly, an explicit consent is required for processing special categories of personal data. Within the app, the collected location data can theoretically reveal this kind of sensitive information on the end users or on other individuals. Therefore, the app developer should acquire the data subjects' consents explicitly in applicable parts. In doing so, the consents can be acquired by electronic means, but the information notices

should be extremely well-organised and specified. If feasible, the app developer should implement a two-stage consent verification system, using an email link and a subsequent verification code.

3. Limitations to the commercial use of location data

3.1. Modern personal data economy, right to be forgotten, and right to data portability

3.1.1. Modern personal data economy

In the online environment, the real value of personal data is connected to the possibilities of third party data usage. Therefore, prudent implementation of the basic data protection principles and lawful acquisition of a legal basis only form the foundation for economically profitable data processing. In this regard, it is necessary to determine which concepts of the data protection framework affect the online data flows including pets' location data. In addition, it is essential to elaborate how the app developer can economically profit from location data by simultaneously respecting the data subjects.

In connection to the app, huge amounts of personal information are constantly transferred between multiple entities.[174] As addressed in the first part of this thesis, advertisers, analytics providers, and other third parties gain access and further benefit from the pets' movement patterns. As a legal problem, *Mäkinen* has defined the context of these online data flows as the *personal data economy*. Traditionally, the data subjects have only limited control over the data transfers including their personal information.[175] In this Sub-Chapter, it is addressed how the role of the data subjects should be enhanced in the modern form of the personal data economy.

The advertisers are the entities which mainly create the actual business opportunity for the online companies processing personal data. By disclosing personal information, the companies increase their income in relation to the relevancy and accuracy of the disclosed data.[176] In 2013, *Financial Times* published a report regarding the real value that the advertisers are generally willing to pay for personal information. According to

[174] Communication COM(2012) 9 final of the European Commission, p. 4.
[175] *Mäkinen* 2013, p. 174 – 179.
Also the European Commission has notified the importance of the European data economy in its Communication COM(2017) 9 final (p. 2).
[176] Mäkinen 2013, p. 180 – 182.

the report, 0,0005 dollars is paid in average for a basic piece of personal information, such as for age, gender, or location of a specific data subject. This means that 0,50 dollars would be paid for the location of 1000 individuals. However, the average value increases with the accuracy of the disclosed information, and therefore, information on planned vacations or on specific purchase interests is worth more than the basic data. If special categories of personal data, such as information on a person's health, are disclosed, the price can increase up to 0,11 dollars per a piece of information.[177] In addition to the report, the digital storage company *Western Digital* conducted a survey in 2015 on the data subjects' general opinion and understanding relating to third party data transfers. In the survey, it was found out that these perceptions vary based on the data subjects' age and gender. Generally, men value their personal data more highly than women, but are more likely to "sell" the information concerned. On the other hand, older data subjects are more reluctant to disclose personal information than younger individuals.[178]

In the context of the pet monitoring app, the profits relating to the online data flows are connected to the amount of the end users. The profits of the app developer are noteworthy only if this amount adds up to tens of thousands of individuals. Otherwise, making the app usage subject to a lump sum or to monthly payments is the best way to profit. If location data is disclosed to the advertisers or to other third parties, the disclosures should always be treated as a separate, not additional and compatible processing purpose. In addition, the disclosures should not contain information included in the special categories of personal data. In this regard, the main challenge is to find a way to include the data subjects in the personal data economy and to increase their knowledge and possibilities to contribute to the data flows.

According to the concept of personal data economy, data protection is primarily recognised as the fundamental right of the end users.[179] In addition, personal data can be defined as *property* to address the problem of unilateral data usage. According to *Saarnilehto*, property is a movable or immovable object, claim, interest, or something immaterial such as patent or copyright.[180] Generally, personal data does not easily fit

[177] *Steel and others* 2013. How much is your personal data worth? Financial Times.
[178] *Curtis* 2015. How much is your personal data worth? The Telegraph.
[179] Article 1 of the Regulation.
[180] *Saarnilehto and others* 2001 – 2017, Chapter I2. Sanomapro online version.

this definition. However, approaching from the economic standpoint, it can be regarded as a non-rival good or a public right, meaning that if someone has access to personal data it does not necessarily preclude further access by someone else.[181] In the Regulation, there is no specific Article which would determine whether personal data qualifies or does not qualify as property. In practice, some online companies, like *Facebook*, use the term '*own*' to describe the relationship between the acquired personal information and the data subjects. In Article 2 of its Legal Terms, *Facebook* claims that all pictures and other content downloaded to *Facebook* will remain property of the users.[182]

In determining personal data as property, both advantages and disadvantages can be identified. According to *Schwartz*, the disadvantages are allocated in three groups, being market failure, public good, and free alienability. *Firstly*, market failure refers to the imbalanced environment within which personal data would be traded. The market would not ensure equal bargaining position for the data controllers and the data subjects. Instead, the data subjects would have only limited control over the offered trading products. Essentially, they should choose between disclosing or not disclosing the information. The market failure would also lead either to over-investing in individuals who do not wish to be contacted or to under-investing in privacy-preserving technology and practices.[183] *Secondly*, personal data should be considered a public good, such as voting rights, clean air, or national defence. Defining personal data as property would lead to undesirable outcomes and cause economic values to override some aspects of the fundamental right.[184] *Thirdly*, free alienability is an important characteristic of property. However, in the context of personal data, restrictions are often imposed on the use of the information. These restrictions include prohibitions to further transfer the data or to process it for other purposes than the original ones.[185]

The advantages associated with determining personal data as property are twofold. *Firstly*, conceptualising personal data in a new way would increase the interest of the data subjects and improve their possibilities to participate in the personal data

[181] *Landes and Posner* 2009, p. 14.
[182] Article 2 of the Updated Legal Terms. Facebook.
[183] *Schwartz* 2004, p. 2076 – 2084.
[184] Ibid., p. 2084 – 2090.
[185] Ibid., p. 2090 – 2094.

economy.[186] As a matter of fact, *Wilhelmsson* has suggested that sufficient flexibility in the field of property law increases the possibilities of legal argumentation and decision-making.[187] Currently, the data subjects might find it extremely difficult to benefit from disclosing personal information. *Secondly*, the constantly changing online environment requires multiple ways to address legal problems. In this regard, property should be defined as a constantly changing concept which dynamically adapts itself to the evolving economic structures.[188] This approach would overcome the fact that legislation is always left behind in relation to the advanced ways to use personal information. Instead of excluding new interpretations, the data protection framework should accept multiple ways of problem-solving. In doing so, defining personal data as property would contribute to better data management and increase the possibilities of data protection.[189]

While monitoring pets' movement patterns, the app developer should primarily treat data protection as the fundamental right of the end users. It should not consider the collected location data as mere property of the individuals. When transferring location data to third parties, the main obligation is to ensure that the end users are included in the personal data economy. In the economic sense, personal data can be defined as a hybrid legal concept which changes its characteristics according to specific situations. As *Pöyhönen* has argued, this approach means that also the relationships connected to the data are asymmetric. '*Asymmetric relationship*' means that an obligation on one hand does not necessarily correspond a right on the other hand.[190] Therefore, the rights of the end users do not limit the obligations imposed on the app developer. In the context of disclosing personal data to the third parties, the adequate level of data protection might require that the end users benefit from the personal data as their property. Nevertheless, applying the hybrid definition does not signify that the app developer can disrespect fundamental aspects of the data protection legislation.

By applying the hybrid legal concept of personal data, the app developer simultaneously ensures that the economic profits associated with the data transfers to the third parties are justified. In other words, the end users most probably accept the significant

[186] *Mäkinen* 2013, p. 192 – 194.
[187] *Wilhelmsson* 2001, p. 194.
[188] *Pöyhönen* 2000, p. 149 – 151.
[189] *Mäkinen* 2013, p. 192 – 194.
[190] *Pöyhönen* 2000, p. 150 – 151.

economic role of the app developer if they are effectively included in the online data flows. In this context, the profits of the end users increase the profits of the app developer.

3.1.2. Right to be forgotten

Chapter III of the Regulation includes fundamental rights granted to each data subject whose personal data is undergoing processing. As concepts, the rights provide the data subjects with effective means to affect the processing of their personal information. The rights are (1) right to information, (2) right to subject access, right to rectification and right to restriction of processing, (3) right to data portability, (3) right to object, (4) right to erasure and right to be forgotten, as well as (5) right related to profiling and automated decision-making. In the economic sense, the rights limit the app developer's possibilities to unilaterally process personal data and encourage the end users to be better informed on the online data flows including their personal information. Especially, the right to be forgotten and the right to data portability directly enable the data subjects to hinder unlimited, exclusive, and unwanted data processing. Subsequently, this Sub-Chapter elaborates the legal implications of the right to be forgotten.

As a concept, the right to be forgotten was not included in the former data protection framework.[191] Currently, it can be exercised against a data controller if the specific exceptions of the Regulation do not apply. In practice, the right should be effectively implemented to the record-keeping and data management operations of the app developer. If not correctly respected, the existence of the right would decrease the economic value of the collected location data. In addition, any insufficiency in compliance would cause damage to the app developer's reputation or decrease the possibilities of further data usage.[192] In order to comply with the right, the app developer should adequately limit the publication of location data by the virtue of data protection.[193] In this regard, the main difficulty is to define which disclosures qualify as making public.

[191] *Carey* 2015, p. 165 – 166.
[192] EU publication. *De Terwangne* 2013, p. 3 – 4.
[193] *Sartor* 2014, p. 2.

In Article 17 of the Regulation, the right to be forgotten is stipulated in connection to the right to erasure. According to Article 17(1), erasure may be requested by a data subject in specific situations, such as if personal data is no longer necessary for the original processing purposes or if a data subject withdraws his or her consent and no other legal basis legitimises the processing. On request, a data controller must erase specified personal information without undue delay.[194] On the other hand, the right to be forgotten applies to situations where a data subject requests erasure pursuant to Article 17(1) and the data controller has previously made the information *public*. During the adoption process of the Regulation, the right faced a significant amount of controversy. Despite the objection, the concept was adopted to the data protection framework to address the potentially unlimited online retention of personal data.[195] According to Article 17(2), the data controller shall respect the right to be forgotten and:

> "*Taking account of available technology and the costs of implementation, -- take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data*."

Following the introduction of the right to be forgotten, legal discussion focused on defining the practical implications of the concept. As an example, *Carey* concluded that there are extensive technical difficulties which the data controllers need to overcome to comply with the right. According to *Carey*, the technical difficulties can be divided into two groups. *Firstly*, it is not clear which kind of actions are included in '*making personal data public*'. *Secondly*, the notifications to the third parties which have gained access to the personal information might require disproportionate effort from the data controller as all recipients may not be easily identified.[196] Furthermore, it is not clear which kind of available technology and costs of implementation are considered proportionate to fulfil the obligation. In addition to *Carey*, also *Kosta* elaborated the practical meaning of the right. According to *Kosta*, the right has special value on the Internet and can be exercised in relation to a data subject who consented to specific data

---

However, as stipulated in Article 17(3) of the Regulation, among other exceptions, the right of freedom of expression and information can prevent a data subject from exercising his or her right to be forgotten.

[194] Article 17(1) of the Regulation.

[195] *Carey* 2015, p. 200 – 201.

[196] Ibid.

processing as a child and wishes later to remove the disclosed information from the Internet.[197]

Even before the right was first introduced, online companies had been pressured to delete public content. However, the deletion had not led to satisfactory outcomes and new legislation was found necessary to solve the problem.[198] According to *Korenhof and others*, there are several reasons to why it has been, and still is, so difficult to effectively delete public content. The main difficulty is simply that once information is published on the Internet, it spreads immediately. Publishing can be done by one click of a mouse, but deleting the data might require contacting indefinite recipients.[199] Therefore, there are no practical means to effectively *forget* someone. As a matter of fact, forgetting refers to the functioning of a human mind and does not fit well the online environment.[200] Instead of forgetting, the right should be defined as an individual's right not to be confronted with his or her past.[201] Furthermore, forgetting is generally connected to old and outdated information. However, in addition to outdated data, the right to be forgotten applies to relatively recent information. For example, this category includes spontaneous and unhesitating posts on online platforms which are later requested to be deleted.[202] Conclusively, the wording of the right is particularly vague. It is not connected to any specific purpose of protection, but instead, the right reflects multiple important concepts recognised in the data protection framework. Among others, these concepts include the right not to be profiled, the right not to be targeted for advertising, and the right not to be seen or discovered by others.[203]

In practice, the data subjects have showed increasing interest in exercising the right to be forgotten. The trend started in 2014, after the Court had issued its decision in the case *Google Spain v Agencia Espanola de Protección de Datos and Mario Costeja Gonzaláles.* By establishing the first form of the right, the Court had ruled that an individual may request an online search engine to delist specific search results connected to the person's name, provided that the information is "*inadequate, irrelevant*

[197] *Kosta* 2013, p. 252 – 254.
[198] *Korenhof and others* 2015, p. 179.
[199] EU publication. *De Terwangne* 2013, p. 3.
[200] *Markou* 2015, p. 211 – 213.
[201] EU publication. *De Terwangne* 2013, p. 1.
[202] Ibid., p. 7.
[203] *Markou* 2015, p. 222 – 223.

or excessive in relation to the purposes of the processing".[204] Following the ruling, requests to be forgotten received by online companies have multiplied. As an example, *Google* has stated that since 2014 it has received more than 650 000 requests. Due to the requests, 43,8 per cent of the URLs concerned have been deleted. In addition, *Google* notes that in determining the need for deletion, it has taken account of the public interest, such as of an individual's public position.[205] Concerning the extent of forgetting, *Google* has deleted search results within the European country search services and on all country search services for queries performed from geolocations which match the requestor's country. Therefore, the deletion has not been conducted internationally.[206]

Within the pet monitoring app, making personal data public could consist of three different types of disclosure, being publication to an indefinite audience, to the end users, or to third party data processors. Here, public means something that relates to or involves people in general, rather than being limited to a specific group.[207] Subject to this definition, Article 17(2) clearly applies to disclosing personal data to an indefinite audience, such as to publishing information on the Internet. However, this kind of data processing is not lawful in the context of the app, and therefore, it is not relevant in determining the special scope of the right to be forgotten. On the other hand, the app developer can make the collected location data available in relation to the end users. For example, this would be the case if the app would transmit communications between the end users or otherwise enable sharing collected data. In this regard, the app would potentially disclose personal data to an indefinite audience, as fundamentally, it would have no real control over the data usage subsequently carried out by the end users. However, having the responsibility to control these data transfers would not be proportionate taking account of the available technology and the costs of implementation. Therefore, the right to be forgotten should not apply to the data transfers to the end users.

[204] Case C-131/12 of the Court, Paragraph 92.
[205] Google's website. Google Transparency Report. URLs deleted from the Google search results based on data protection.
[206] *Bertram and others* 2018, p. 3. Google.
[207] Cambridge Dictionary. Definition of '*public*'.

During the preparatory works of the Regulation, the European Parliament proposed to widen the wording of Article 17(2) to include both transferring and making public.[208] According to the Parliament, transferring was meant to signify disclosing or making available, such as assigning data to third party data processors.[209] Nevertheless, the final wording of the Article includes only making personal data public and does not mention third party data transfers. This choice of wording is reasonable, as the relationship of a data controller and its data processors is primarily stipulated in Article 28. According to this Article, each data controller has the obligation to ensure that all data processors under its control respect the data subjects' fundamental rights, such as the right to be forgotten. Therefore, despite the final wording of Article 17(2), disclosing personal information to the data processors should be treated as making personal data public. On request, the app developer should inform each relevant data processor. In addition to Articles 17(2) and 28, also Article 19 addresses the obligation to inform pursuant to Article 17(1). The app developer should inform each recipient to whom the personal data has been disclosed, unless notifying proves impossible or involves disproportionate effort. In this regard, the main difficulty is tracking transfers from the European Economic Area to any third country.[210]

As a final consideration, compliance with the right to be forgotten is practically an obligation to control the disclosure chains including pets' location data. The concept does not require that the app developer effectively ensures that all relevant information is effectively erased, but that the third parties are adequately notified.[211] Essentially, the right to be forgotten limits the online data retention periods and reinforces the end

---

[208] Report of the European Parliament on the Proposal for the Regulation (*Proposal of the European Commission for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (COM(2012) 11 final, the Proposal for the General Data Protection Regulation)) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), Opinion of the Committee on the Internal Market and Consumer Protection, Amendment 120.

[209] EU publication. *De Terwangne* 2013, p. 11.

[210] Chapter V of the Regulation.
In the Regulation, these kinds of data transfers are prohibited, unless the third country or international organisation concerned provides an appropriate level of protection for the rights and freedoms of the data subjects (*Carey* 2015, p. 133 – 134).
According to Articles 45 and 46 of the Regulation, the appropriate level of data protection can be based either on an adequacy decision of the European Commission (Adequacy decisions. The European Commission, ec.europa.eu) or on appropriate safeguards provided by the data controller or data processor. If personal data is lawfully disclosed internationally, it should be possible for the app developer to comply with a specific request to delete also regarding these transferred pieces of information.

[211] EU publication. *De Terwangne* 2013, p. 11.

users' position in the personal data economy. Due to the right, location data may not be held as an exclusive economic asset or traded freely in the context of a business transaction.[212]

3.1.3. Right to data portability

Data portability means a right to receive personal data that has been provided to a specific data controller and that undergoes processing by automated means.[213] The existence of the right signifies that the data subjects fundamentally decide which entities gain access and economically profit from the online data flows including their personal information. For the pet monitoring app, data portability imposes an obligation to maintain a system to answer portability requests. In other words, the end users must be able to easily change service providers without hindrance on the part of the app developer.[214]

The essence of data portability is that personal data must be receivable in a commonly used, machine-readable format[215] and transmittable to another data controller.[216] As a limitation, executing the right should not affect the protection for the data subjects' other fundamental rights and freedoms.[217] Despite its novelty, the right remains further unexplained in the Regulation.[218] In relation to the app, the specific requirements for system interoperability, identifying requesting end users, and ideal format of portable data need to be construed in practice.[219]

---

[212] Ibid., p. 3 – 4.
According to *Kremer* 2016 (p. 137), the fundamental rights of the data subjects, such as the right to be forgotten, have a significant effect on business operations.
[213] Article 20 of the Regulation.

[214] *Kremer* 2016, p. 138.
[215] According to Recital 21 of the Directive 2013/37/EU, "*a document should be considered to be in a machine-readable format if it is in a file format that is structured in such a way that software applications can easily identify, recognize and extract specific data from it. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats*".
[216] Article 20 of the Regulation.
[217] Guidelines of the Working Party on the right to data portability 242 rev.1/2016, p. 7 – 8.
Particularly, the right to data portability needs to be in balance with the right to be forgotten. Moreover, the storage limitation principle may not be disregarded by the virtue of data portability (*Bapat* 2013, p. 2).
[218] *Carey* 2015, p. 201.
[219] *Kallasvuo* 2015, p. 154.

According to the Working Party, a fundamental characteristic of the right to data portability is that the concept is divided into two distinct parts. The data subjects have both the right to receive data that they have provided to a specific data controller and the right to transfer the information to another service provider. *The right to receive* is closely connected to the right to subject access and gives the data subjects the possibility to extend the scope of the basic access and to retain personal information for future purposes.[220] On the other hand, *the right to transfer* signifies that a data subject may request personal data to be transferred directly between two data controllers[221] or through the data subject. For the data controllers, this second part creates the obligation to develop interoperable formats which contribute to the smooth functioning of the right. The data controllers are not obliged to have universally compatible data storage or transfer systems[222], but the format structures must hinder unilaterally profitable *data lock-ins*.[223] In doing so, data portability increases the data subjects' possibilities to engage in the personal data economy.[224]

As a concept, data portability is related to the data management model called *MyData*[225]. Like defining personal data as property, the model aims at restoring the control over the personal information on the actual data subjects and requires that the data subjects effectively benefit from disclosing it. Applying the model does not signify that personal data should be considered a mere economic concept, but that it has also research-related, historical, and statistical value. The focus should be on the factual control and data management possibilities.[226] As opposed to the *MyData* model, the scope of data portability in the Regulation is limited to information provided to a data controller by a data subject.[227] This limitation precludes all inferred information which has been subsequently created by the data controller. Therefore, *observed information* such as activity logs or browser history are included in data portability, but *inferred information* such as health or risk management profiles based on an assessment on the

[220] *Bapat* 2013, p. 1.
[221] According to Article 20(2) of the Regulation, the obligation to transmit personal data to other data controller applies only where technically feasible.
[222] According to Recital 68 of the Regulation, the data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the data controllers to adopt or maintain processing systems which are technically compatible.
[223] Guidelines of the Working Party on the right to data portability 242 rev.1/2016, p. 5.
[224] Ibid., p. 4 – 8.
[225] According to *Kallasvuo* 2015 (p. 144), the *MyData* model was first adopted by the UK government in 2011.
[226] Ibid., p. 144 – 146.
[227] Article 20 of the Regulation.

part of the data controller are not. Furthermore, data formed in the personalisation, recommendation, categorisation, or profiling processes do not normally fit the definition. These limitations significantly decrease the data subjects' data management possibilities and complicate the process of identifying information included in data portability.[228] Due to these shortcomings of Article 20, the *MyData* model is not fully respected in the Regulation.

As specified above, the requirements not sufficiently explained in the Regulation concern system interoperability, identification of requesting data subjects, and ideal format of portable data.[229] In this context, the main issue for the app developer is that a *contextually interoperable system* may not be regarded as interoperable on the part of another service provider. In practice, this kind of compatibility problem can make a contemplated data transfer impossible or otherwise too expensive to execute.[230] In addition, before implementing data portability, the app developer should ensure that the requesting end user is *identified*. In doing so, the data controller faces problems like in the context of the wish indication requirement for valid consent. The identification should not lead to significant further data processing or hamper the app usage. As an example, the fingerprint technology or a specific email verification system can provide sufficient proof.[231] Regarding the *form and amount of portable data*, the difficulty is that the app developer might in some cases provide overlapping and unnecessary information not relevant for the receiving data controller. Here, the legal issue is that the recipient is limited by its data processing purposes and overlapping does not allow it to gain access to the unnecessary information.[232]

In practice, the app would most probably manage the right to data portability through the APIs of the operating mobile devices. This automated system would decrease the organisational burden to comply with the right and make it possible for the end users to independently access and receive personal data.[233] Economically, managing data portability through the APIs is a feasible way to comply with the right as making a portability request subject to a fee would be unlawful almost always. This rule applies,

---

[228] Guidelines of the Working Party on the right to data portability 242 rev.1/2016, p. 9 – 11.
[229] *Kallasvuo* 2015, p. 154.
[230] Ibid.
[231] Guidelines of the Working Party on the right to data portability 242 rev.1/2016, p. 13 – 14.
[232] Ibid., p. 6.
[233] Ibid., p. 15 – 16.

unless the app developer demonstrates that a specific request is manifestly unfounded or excessive.[234] Here, the costs of implementation or the overall amount of the requests do not affect the definition of excessive. [235] In the online environment, data portability can hardly ever be refused, even in the case of frequent requests.[236] In addition, the app developer as an information society service operator should provide portability in a relatively short time frame which even in the case of demanding requests is required to be clearly less than a month.[237]

Finally, despite the ambiguous goals of data portability, implementing the right might prove difficult in practice. Especially, the app developer might find it impossible or too expensive to create universally interoperable data storage systems. From the end users' standpoint, data portability opens harmful data lock-ins. From the app developer's standpoint, it complicates defining the commercial value of location data. In a business transaction, data portability might hamper the free movement of location data and decrease the data usage possibilities during the post-closing phase.[238]

3.2. Personal data in a private corporate acquisition process

3.2.1. Disclosing personal data in the modern due diligence process

After the contextual economic concept of personal data is defined and the implementation of the data subjects' rights is adequately managed, economically profitable data processing within the app requires further that a transfer to a third party is structured in a legal way. In this regard, it is normal for the budding startup company to be at some point acquired by an industrial buyer or a private equity investor.[239] Therefore, addressing the problem of location data transfers in a corporate acquisition process is necessary to comprehensively understand how a profitable data transfer is organised in relation to the app.

---

[234] Article 12(5) of the Regulation.
[235] This provision includes protection for trade secrets, confidential information, and intellectual property rights in the context of data portability. Despite the required resources and investments in IT, the costs of the new technologies may not be compensated by a fee from the data subjects (*Bapat* 2013, p. 2).
[236] Guidelines of the Working Party on the right to data portability 242 rev.1/2016, p. 15 – 16.
[237] Ibid., p. 14.
[238] According to *Bapat* 2013 (p. 2), "*this freedom and choice will -- lead to increased competition between service providers and ultimately secure better value for money*".
[239] *Lauriala* 2013, Chapter 1.1 Yristysostajat. Sanomapro online version.

This Chapter addresses how pets' location data is legally transferred during the modern corporate acquisition process and which data protection obligations limit the free movement of the personal information. [240] Firstly, the difficulty to transfer the personal data during the modern due diligence process is elaborated in this Sub-Chapter. As a rule, no personal data should be revealed to a buyer candidate without a relevant legal basis. To disclose modified documents including hidden personal information, the app developer can use one of three specific methods. These methods are concealing personal information (redaction), anonymisation or pseudonymisation, and model documentation.

In general, '*corporate acquisition*' is a business transaction which is characterised by the transaction model where an industrial buyer or private equity investor acquires a specific target company.[241] Conceptually, corporate acquisitions can be allocated in multiple ways, approaching either from a strategic or executive standpoint. *Strategically*, a corporate acquisition can be horizontal, meaning that a company increases its market share by buying a competitor[242], or vertical, meaning that the transaction orientates towards a different stage of a production cycle inside the same market[243]. In addition, strategic corporate acquisitions can be concentric or conglomerate.[244] *Executively*, corporate acquisitions can be allocated in business (asset) acquisitions, share acquisitions, and mergers. The target of a business acquisition comprises of certain assets constituting an independent economic entity. For example, the entity can be a company's profit centre or production line. On the other hand, share acquisition means purchasing all or some of a target company's shares.[245] Finally, a merger is "*a combination of two corporations in which only one corporation survives and the merged corporation goes out of existence. In a merger, the acquiring company assumes the assets and liabilities of the merged company*".[246]

---

[240] According to *Aukia* 2018 (p. 11), data protection has become increasingly relevant in the context of corporate acquisition and capital investments.
[241] Financial Dicitionary. Definition of '*M&A*'.
[242] *Lauriala* 2013, Chapter 2.1 Yristyskauppojen strategian mukainen jaottelu. Sanomapro online version.
[243] Financial Dicitionary. Definition of '*vertical acquisition*'.
[244] According to *Lauriala* 2013 (Chapter 2.1 Yristyskauppojen strategian mukainen jaottelu), in a concentric corporate acquisition the buyer's line of business is different than the target company's line of business, but the market, marketing, and distribution channels, or the technology and research functions are similar. On the other hand, a conglomerate corporate acquisition orientates to a completely new market.
[245] *Lauriala* 2013, Chapter 2.2 Yristyskauppojen toteutustavan mukainen jaottelu. Sanomapro online version.
[246] *Gaughan* 2010, p. 12.

As a process, a corporate acquisition is divided into multiple stages. *During the first stage*, an acquiring company creates its acquisition strategy and defines which kind of deals would favour its business and boost its operations. This stage also includes searching interesting target companies and evaluating their capabilities to contribute to the already existing business model. Once an interesting target is found, the acquiring company often determines a preliminary purchase price that will later be adjusted according to the findings of the acquisition process.[247] *In the second stage*, the actual negotiations on the final transaction structure begin. Depending on the type of the negotiations, this stage can include only the target company and one buyer candidate, or alternatively, multiple buyer candidates. Therefore, the second stage can be either a direct negotiation between two parties, a limited auction between the target and certain buyer candidates, or a public auction open to all interested buyers. The negotiation type will normally be determined by the target company's willingness to publish its intention to be sold.[248] Furthermore, the second stage includes planning on the exact transaction structure, as well as drafting of specific non-disclosure agreements, letters of intent, and memorandums of understanding. As a simultaneous phase, one or multiple acquiring companies (and often also the target company) conduct due diligence.[249] Finally, *the third stage* of a corporate acquisition process is divided to the execution, implementation, and post-closing management of the deal.[250]

As presented above, due diligence is one of the steps included in the second stage of a corporate acquisition process. By definition, due diligence is the process of assessing the merits, issues and risks relating to the business transaction. In due diligence, information on the target company is prudently collected and processed to increase knowledge on its operations.[251] In doing so, the financial, management, and operational conditions of the company are critically analysed.[252] Traditionally, a well-executed due diligence includes three different standpoints. *From the business standpoint*, the acquiring company or companies evaluate the target company's management team and resources, as well as identify and evaluate its customers and relevant markets. *From the financial standpoint*, the target company's accounting books and other available

[247] *Lauriala* 2013, Chapter 3. Yristyskauppaprosessi ostajan näkökulmasta. Sanomapro online version.
[248] Ibid., Chapter 4. Yristyskauppaprosessi myyjän näkökulmasta. Sanomapro online version.
[249] *Mäkelä* 2011, p. 118.
[250] *Lauriala* 2013, Chapter 3. Yristyskauppaprosessi ostajan näkökulmasta. Sanomapro online version.
[251] *Crilly and Sherman* 2010, p. 23.
[252] *Lauriala* 2006, p. 2 – 3.

financial data are appropriately examined. Furthermore, *from the legal standpoint*, the target company's ownership structure, its ownership in other entities, and any legal claim relating to it are identified.[253] Regarding the acquisition of a startup company, due diligence should be executed with extreme care and precision in order to recognise possible risks and issues associated with the contemplated transaction.[254]

In addition to the three traditional due diligence standpoints, data protection and other IT-related issues have become an integral part of the modern due diligence process. This new standpoint requires that an acquiring company carefully inspects the target company's compliance with relevant data protection legislation and identifies shortcomings in its data processing methods or system robustness. Furthermore, the new standpoint signifies that while providing information to a buyer candidate before the deal execution, the target company should not reveal any personal data without a relevant legal basis. In practice, this prohibition concerns almost all business transactions, as all target companies normally process at least customer and employee related personal information.[255] Regarding the pet monitoring app, the prohibition imposes a limitation to granularly disclose pets' location data during a transaction process.

Technically, the due diligence process is managed in a private or third party data room. A virtual third party data room service is a platform on which the parties to a business transaction can exchange information securely and confidentially. The virtual data room is an online portal, where both the target company's representatives and the buyer candidates' representatives can download necessary material. In the data room, the downloaded information can be simultaneously accessed and coherently referred to in the due diligence reports. If no third party service is used, a data room can also be a privately operated virtual platform or an actual physical location available to the parties to the transaction.[256] If a third party service provider is chosen, a specific data protection agreement should be entered into to sufficiently regulate the service provider's data

[253] Ibid., p. 3.
[254] Ibid., p. 4.
Mäkelä 2011, p. 119.
[255] *Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman.
[256] Merrill Corporation's website. What Is a Virtual Data Room (VDR)? Merrill is one example of an international third party data room service provider.

protection obligations.[257] These obligations should include adequate security measures regarding downloaded information and general practices on returning the data after the transaction.[258] As a matter of fact, a third party data room service provider qualifies as data processor in the meaning of the Regulation.

Regarding the information provided to a data room in a corporate acquisition process, the app developer can use three different methods to avoid the illegal disclosure of personal data. As mentioned above, these methods are concealing personal information (redaction), anonymisation or pseudonymisation, and model documentation.[259] In addition to the documents modified according to the methods, original versions including personal information can also be downloaded where technically feasible. Here, '*technical feasibility*' means that the chosen data room allows granting access only to the relevant data controllers.[260] As opposed to avoiding the disclosure of personal data, the end users can also be asked to provide their consents to the disclosure during the transaction. However, acquiring all necessary consents requires often unreasonable effort, and in doing so, reveals the existence of the transaction and hampers its confidentiality.[261] Therefore, the best practice is to hide all information relating to identifiable individuals.

Depending on the amount of documentation, concealing is a relatively time-consuming way to hide personal data. Normally, concealing means that documents are manually redacted.[262] Technically, the app developer should redact documents by an appropriate tool which not only permanently deletes underlying text and images, but also all metadata attached to them. On the other hand, redaction cannot be conducted by merely drawing black boxes on top of personal information. This kind of implementation enables the recipients to later copy and paste the data below the boxes.[263] Nevertheless, redaction is not the primary way for the app developer to hide pets' location data.

---

[257] *Maxwell and others* 2015, p. 3. Data protection in M&A transactions: A how-to-guide. Hogan Lovells.
[258] *Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman.
[259] Ibid.
[260] ShareVault's website. How to redact text or images in a PDF. ShareVault is another example of an international third party data room service provider.
[261] *Maxwell and others* 2015, p. 3. Data protection in M&A transactions: A how-to-guide. Hogan Lovells.
[262] According to Merriam-Webster Dictionary, '*redaction*' means obscuring or removing information from a document prior to publication or release.
[263] ShareVault's website. How to redact text or images in a PDF.

Instead, the method should be used in a corporate acquisition process to disclose relevant employment contracts, customer agreements, and similar documents.

Anonymisation and pseudonymisation were already addressed in Sub-Chapter 2.2.2.3.. Essentially, they are techniques to modify personal data in a way which no longer permits the recipients to identify specific individuals.[264] Anonymisation in the context of pets' activity profiles means that a profile cannot be connected to a specific location, pet or end user. Instead, anonymised documents only present generic activity profiles which help a buyer candidate to understand the basic operations of the app. Unlike anonymisation, pseudonymisation leaves the "key" to unlock the pseudonymised information in the possession of the app developer.

The third way to disclose sensitive information during due diligence is to transform documents including personal data into model agreements, summaries, or statistical charts. This kind of practice reveals general information on a target company's fundamental characteristics and technology, but leaves individual aspects and information hidden.[265] For the app developer, model documentation works in a similar way than anonymisation and pseudonymisation. On the down side, overly general information is often not specific enough to fulfil the informational requirement of a buyer candidate conducting exhaustive due diligence.[266] Therefore, the app developer can prefer anonymisation or pseudonymisation to disclose modified activity profiles.

3.2.2. Data protection risks and risk management

As presented above, the foundation of a successful corporate acquisition process is well-structured due diligence. From the data protection standpoint, no personal data should be illegally transferred prior to the execution of the transaction. Taking the premise further, this Sub-Chapter focuses on determining which kind of personal data related shortcomings can be identified during the modern due diligence process and how these identified risks should be addressed in the final asset purchase, share purchase, or merger agreement. In this regard, the main personal data related considerations

[264] *Chen and others* 2017, p. 8967.
[265] *Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman.
[266] *Crilly and Sherman* 2010, p. 23.

associated with the app are the applicable data protection legislation as well as compliance with relevant data protection obligations arising from this legislation. Especially, all data processing conducted within the app should have a legal basis and all collected location data should be sufficiently protected.

In detail, the main data protection risks identifiable in due diligence relating to the app are twofold. *Firstly*, the app developer should be able to demonstrate that the end users' consents are legally acquired, and *secondly*, that the basic data protection principles are prudently implemented to its data processing practices. In other words, the end users' consents should fulfil all requirements stipulated in the Regulation and the basic principles should be coherently respected. Among others, monitoring these aspects includes evaluating the provided information notices, assessing any third party contractual obligation, as well as ensuring sufficient internal record-keeping and security measures.[267]

In general, data protection risk management in the modern due diligence process should begin by determining all relevant jurisdictions. In addition to the data protection framework, multiple national and international legislative layers can affect the operations of the app. Especially in the online environment, data processing normally has a strong international aspect and data subjects in third countries are commonly targeted. These factors complicate defining applicable legislation and increase the scope of required due diligence.

In Europe, the Regulation primarily determines the relevant data protection risks in a corporate acquisition process. The Regulation applies to the operations of the data controllers and data processors with an establishment in the EU, regardless of where the actual processing takes place. Additionally, the Regulation applies to the data controllers and data processors not established in the EU, if the data subjects are in the EU and the processing relates to offering of goods or services in the EU or to monitoring the data subjects' behaviour that takes place in the EU.[268] This territorial scope is extensive and makes defining applicable legislation much more difficult than just identifying the jurisdiction under which the target company has been

[267] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[268] Article 3 of the Regulation.

incorporated.[269] Furthermore, despite the fact that the Regulation has harmonised data protection in the EU, many aspects of protection are still subject to national discretion, which increases the legislative variety.[270] Despite the possibility of the accumulative legislative layers, this Sub-Chapter only focuses on the data protection obligations which the data protection framework imposes on the app developer.

After determining the applicable legislation, data protection due diligence should focus on the specific legal obligations. Regarding the app, a buyer candidate should verify that the consents acquired from the end users fulfil all legal requirements. Especially, it should ascertain that the app provides adequate and necessary information notices to the end users prior to processing or gaining access to any location data. As recommended by the Working Party, these notices should be provided in a granular structure. If not ambiguous, they can include a privacy policy[271] forming the second or third layer of the structure.[272] On the basis that privacy policies are often extremely detailed and comprehensive, a buyer candidate should ensure that the app's policy includes only information which is required in the data protection framework or is otherwise necessary. If the app has different privacy policies applying to different data subjects, all relevant policies should be evaluated. As an example, this is the case if a former privacy policy is associated with consents which were acquired before the adoption of the current policy. Moreover, it should be ascertained that all current and former privacy policies comply with other layers of their relevant information structure.[273] A further risk relating to a privacy policy of the app is that the policy can contain privacy clauses which are technically impossible or very difficult to maintain with limited privacy resources. This kind of shortcoming can later lead to surprising data protection liabilities, such as to significant administrative fines.[274]

In addition to the information notices, third party contractual obligations are a fundamental aspect of data protection due diligence. These obligations commonly arise from contracts with advertisers and other third parties. In this context, the app developer

[269] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Privacy Due Diligence: Key Areas of Inquiry. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[270] Recital 8 of the Regulation.
[271] *Kosta* 2013, p. 215 – 218.
[272] Opinion 10/2004 of the Working Party, p. 8.
[273] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Privacy Due Diligence: Key Areas of Inquiry. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[274] Ibid.

might be subject to further privacy policies and similar data protection liabilities. As a possible risk, the contractual obligations can be too vague and leave unjustified freedom for the third parties to determine fundamental aspects of the data processing.[275] Within the app, relevant third party contractual obligations should be examined at least in relation to the advertisers, cloud service suppliers, and app stores. Especially, the app stores often base their operations on specific policies that must be complied with when using the platform.[276] Regardless of whether the app developer has only marginal control over the third party contractual obligations, inferred liabilities can directly affect the value of the location data in a corporate acquisition process.[277]

Furthermore, ensuring sufficient internal record-keeping and security measures is necessary in exhaustive data protection due diligence. This aspect is connected not only to the consent requirement, but also to the efficient implementation of the basic data protection principles. For the verification of consents acquired by the app, a buyer candidate should ensure that sufficient information is recorded on the sessions in which the consents of the end users are expressed. In addition, the app developer should be able to provide documentation on the specific consent workflows and copies of the information notices.[278] In order to evaluate security measures, a buyer candidate should be able to verify that the app developer has implemented standard cryptography and other privacy-preserving techniques which adequately protect the rights and freedoms of the individuals during locating and while information is transferred between the electronic collars and the operating mobile devices. As an example, absence of a breach procedure automatically renders the app a risky target.[279] Finally, a well-informed buyer candidate should evaluate the recorded and practical level of security. In this regard, it should take account of the possibility of data breaches and locating inaccuracy regardless of the protective measures.

In the final asset purchase, share purchase, or merger agreement, the above identified risks should be reflected in the data protection warranties, representations, and

[275] Chapter V of the Regulation.
[276] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Privacy Due Diligence: Key Areas of Inquiry. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[277] *Carey* 2015, p. 266 – 267.
[278] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 20.
[279] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Privacy Due Diligence: Key Areas of Inquiry. Harvard Law School Forum on Corporate Governance and Financial Regulation.

indemnities.[280] Another possibility to mitigate risks in a corporate acquisition process is to manage any shortcoming during the process. If a data protection warranty, representation or indemnity is found necessary, it should be sufficient to protect the buyer from all reasonable data protection liabilities.[281] The clause should not be formulated to cover only general compliance with laws, as normally, this kind of protection would be limited to a relatively short time period (such as to a year prior to the transaction). Instead, the warranty, representation or indemnity should cover a comprehensive area of privacy, including laws, contractual obligations, industry-standards, enforcement actions, and privacy-related complaints. In addition, the target company's obligation to disclose privacy related information should be reinforced.[282]

If the relevant data protection risks would not be managed in the final agreement or during the process, the effects of data breaches and similar data protection threats would become a subsequent risk for the buyer. Moreover, the most important consequence of a data protection shortcoming is often damage to the buyer's reputation, loss of clients, or harmful disruption in business. Moreover, the Regulation grants the supervisory authorities the right to block data processing conducted on illegally accessed data. This authorisation signifies that personal data incautiously transferred in a corporate acquisition process might not be later used by the buyer.[283] The above identified aspects are extremely relevant in an acquisition process concerning the app, as the transferred data and related systems can work as an attack pathway for malicious third parties and provide access to the buyer's databases.[284] Therefore, adjusting the final purchase price according to the real value of the location data does not often suffice to protect the buyer as damage to the buyer's reputation is far more harmful than financially compensating a specific shortcoming. Instead, a data protection warranty, representation or indemnity is the best way to mitigate identified risks in an acquisition process.

---

[280] According to *Chapman* 2015 (Warrranties, Representations and Idemnities), *"a warranty is a statement or promise in a contract that something is or will be true*". If a party to whom the statement or promise was made suffers loss, "the innocent party" has a contractual claim for damages. On the other hand, *"a representation is a pre-contract statement made to a party to a contract, as a result of which that party is induced into entering into the contract. If a representation turns out to be incorrect, the buyer may be able to sue for mispresentation*." Finally, *"an indemnity is simply a promise to pay losses or damage suffered by another party*" (all financial consequences).

[281] *Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman.

[282] *Ilan* 2016. Privacy in M&A Transactions: Pre Closing Liabilities. Privacy-related Representaions in M&A Agreements. Harvard Law School Forum on Corporate Governance and Financial Regulation.

[283] *Aukia* 2018, p. 12.

[284] *Maxwell and others* 2015, p. 4. Data protection in M&A transactions: A how-to-guide. Hogan Lovells.

3.2.3. Data integration

The purpose of transferring personal data in a corporate acquisition process is to later integrate the data to the buyer's databases and to enable further usage in the buyer's business operations. In addition, the fundamental purpose for the target company is to get the best possible compensation for the transferred personal data. Normally, shortcomings in the data integration possibilities decrease the value of the personal data and increase the IT expenses on the buyer's side.[285] Therefore, it is crucial to elaborate how the data integration should be structured in a corporate acquisition process concerning the app. In this regard, the most noteworthy aspects to consider are pre-closing integration, deal structure, and compatibility of the buyers and the app developer's data protection practices.

In principle, signing of an asset purchase, share purchase or merger agreement does not signify that the deal is finalised and will remain enforceable. Instead, subsequent closing of the deal might depend on various factors possibly realising in the future.[286] Therefore, personal data should be disclosed and *integrated during the pre-closing phase* only if it is necessary for the deal execution and does not amount in inadequate or excessive data processing. In addition, the data transfer should be lawful and comply with Article 6(1) of the Regulation. Particularly, the data transfer should be based on consent, contract performance, or legitimate interest. These requirements are further addressed below.

As already mentioned in Sub-Chapter 3.2.1., acquiring *consents* from the data subjects whose personal data is transferred in a corporate acquisition process is often not feasible. In general, this legal requirement should be relied upon only if the number of the data subjects is small and the individuals concerned have a specific need to be aware of the contemplated transaction. Otherwise, reliance on consent endangers the confidentiality of the transaction. Most probably, this would be the case also in an acquisition process concerning the app. On the other hand, the *contract performance* requirement mainly applies to situations where important customer or similar agreements are transferred during the pre-closing phase. These agreements may be

[285] Ibid., p. 5.
[286] *Aava* 2010, p. 33 – 34.

fundamental to a target company's operations, and therefore, an important source of information.[287] In the context of the app, contract performance does not allow the app developer to transfer identifiable location data prior to closing.

In practice, the *legitimate interest* requirement has been frequently used to disclose personal data pre-closing. However, to lawfully rely on the requirement, the buyer's legitimate interest to receive personal data should be in balance with the fundamental data protection rights and freedoms of the data subjects.[288] In other words, the mere existence of a business transaction does not signify that a legitimate interest to transfer personal data exists. As a basic rule, the requirement can be relied upon if most requirements for closing are fulfilled.[289] Normally, the app developer is not able to transfer the pets' location data during the pre-closing phase in a legitimate interest. As addressed above, the buyer's informational requirement can be sufficiently fulfilled by using anonymised or pseudonymised documents, model profiles, or similar non-identifiable formats.

After closing, all personal data relevant in a transaction are transferred to the buyer. In this regard, the lawfulness of the disclosure depends on *the chosen deal structure*. In the case of a basic share purchase[290], the operations of the target company remain unchanged. If no personal data is integrated to the existing databases of the buyer and if the data processing is continued for the original processing purposes, reliance on a legitimate interest is sufficient to legally execute the data transfer. Within the app, this means that the end users are merely informed on the corporate acquisition and offered the possibility to opt-out. As opposed to the basic share purchase, relying on a legitimate interest in a share purchase including integration, merger or asset purchase[291] might not be lawful. In these contexts, the extent of the original consents should allow the location data to be transferred, and the provided information notices should have

---

[287] *Ilan* 2016. Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities. Risks Associated with Transferring or Disclosing Target's (or Seller's) Personal Data to Purchaser. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[288] Recital 47 of the Regulation.
[289] *Ilan* 2016. Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities. Risks Associated with Transferring or Disclosing Target's (or Seller's) Personal Data to Purchaser. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[290] For example, this is often the case when a private equity investor the acquiring company.
[291] Due to an asset purchase, the buyer normally becomes a new data controller for the transferred personal data (*Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman).

included accurate clauses allowing the disclosure in a corporate acquisition process.[292] Moreover, the end users should still be informed on the transfer and provided with the possibility to opt-out. If the transfer disproportionately affects the rights and freedoms of the end users, new opt-in consents are required. This is the case if the transfer is made to a completely different field of business.[293]

After the lawfulness of the data disclosure in an acquisition process is ensured, effective post-closing integration still requires that *the buyer's and the target's data protection practices are compatible*. If the privacy policies, third party contractual clauses, data storage and encryption standards, processing purposes, as well as other similar practices do not correspond to a certain degree, the buyer might be unable to combine previously owned and newly acquired data. This kind of compatibility problem can be managed in relation to the app by bringing the app developer's lower privacy standards to the same level with the buyer's requirements or by lowering the protection granted in the app developer's policies. In practice, the only feasible way is increasing the level of protection as lowering normally has a negative effect on the buyer's reputation and relationships with its clients. However, increasing the level of protection most probably implies significant costs. In addition, any fundamental changes to the processing purposes require that new opt-in consents from the end users are acquired. As an alternative, the transferred personal data can also be processed as an independent entity without integration. However, this possibility is often not ideal for the buyer's business.[294] Therefore, the data integration challenges should be identified during due diligence and avoided where technically possible.

3.3. Synopsys

In the second part of this thesis, it was determined how the economic value of location data is connected to the possibilities of third party data usage. In this regard, the second part focused on three different topics, being the economic definition of personal data,

[292] *Ilan* 2016. Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities. Risks Associated with Transfers at Closing. Harvard Law School Forum on Corporate Governance and Financial Regulation.
[293] *Lindroos and Walkjärvi* 2016. How to take Data Protection into Account in M&A Transactions – 6 Tips. Castrén & Snellman.
[294] *Ilan* 2016. Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities. Risks Associated with Post-Acquisition Integration of Personal Data. Harvard Law School Forum on Corporate Governance and Financial Regulation.

the data usage limitations posed by the right to be forgotten and the right to data portability, as well as the practical difficulty to transfer location data in a private corporate acquisition process. In the context of the first topic, personal data was defined as a hybrid legal concept, fundamentally allowing it to be considered as property of the data subjects. On the other hand, the second topic was chosen to identify how the rights significantly affect the commercial value of personal data. Subsequently, it was reflected within the third topic how this commercial value is realised only if personal data is transferred in a legally structured way. This Sub-Chapter summarises the main findings connected to the topics.

Traditionally, only the data controllers have profited from the data transfers to the advertisers or to other similar third parties. Currently, these unilaterally beneficial relationships are not considered sustainable, and therefore, the app developer should treat the end users as important actors in the modern personal data economy. In other words, *personal data is a hybrid legal concept* which effectively adapts itself to specific data protection situations. Where necessary, personal data is defined as property of the end users. Here, personal data is a non-rival good or a public right, meaning that the rights and obligations connected to the data might not be in balance. Economic rights of the end users do not limit the legal obligations imposed on the app developer.

The right to be forgotten is a supplementary concept to the classic right to erasure and was first introduced to the data protection framework in the Regulation. The right has special value on the Internet where forgetting uploaded information is often impossible. In practice, forgetting means limiting the publication of location data by the virtue of data protection. For the app developer, the main difficulty associated with the right is to determine the meaning of '*making public*'. As argued in Sub-Chapter 3.1.2., the app developer should at least consider public all disclosures to third party data processors.

The right to data portability provides the data subjects with the possibility to easily change service providers. The right is divided both to the right to receive and to the right to transfer. Portability increases the data subjects' data management and control possibilities, and reflects the specific *MyData* model. On the down side, portability applies only to observed information and cannot be exercised in relation to inferred data. For the app developer, the main difficulty connected to data portability is to develop interoperable systems. In addition, the app developer must identify the

requesting end users and determine the ideal format of portable data. Conclusively, if the right to data portability is adequately respected, the app developer cannot treat location data as an exclusive economic asset.

The modern corporate acquisition process is divided into multiple phases. Data protection due diligence is included in the second phase of the process. During data protection due diligence, the app developer should not disclose identifiable location data to a buyer candidate. Documents including personal information should be concealed (redacted), anonymised or pseudonymised, or transformed into model documentation. With the modified documents, a buyer candidate can sufficiently identify the relevant legislation applying to the app as well as evaluate the provided information notices, third party contractual clauses, and internal security measures. Based on the findings of data protection due diligence, the identified risks should be managed in the final asset purchase, share purchase, or merger agreement. In detail, the risks should be reflected in the data protection representations, warranties, or indemnifications, covering a comprehensive area of privacy. Otherwise, a data protection shortcoming can result into damage to the buyer's reputation, loss of clients, or harmful disruption in business.

After the fulfilment of all requirements for the closing of a corporate acquisition process, the location data acquired within the app can be transferred to the buyer. Subsequently, the buyer can integrate the data to its databases and use it in its business operations. In this regard, the chosen deal structure determines whether new consents from the data subjects are required. Finally, appropriate data integration is possible only if the buyer's and the app developer's data protection practices are compatible to a certain degree.

4. Conclusions

4.1. Over-valuing consent

For the app developer, consent is the main way to legalise the collection of pets' location data. However, consent should not be considered the sole sufficient basis to protect the fundamental rights and freedoms of the end users.[295] In the Regulation, data protection is an overall obligation. Therefore, only comprehensive data protection respecting the entire data protection framework protects the app developer from administrative sanctions and other data protection liabilities. Instead of the consent requirement, more fundamental data protection obligations in relation to the app can be argued to be the implementation of the basic data protection principles and sufficient record-keeping.

Most of the obligations imposed in the Regulation were already present in the former data protection framework. The new legislation has mainly increased the administrative sanctions and made data protection an intriguing concept of legal discussion. Previously, many enterprises had not taken account of the applicable legislation, and subsequently, their data protection practices were left 20 years behind.[296] In general, the obligations of the data protection legislation have applied and still apply to almost all private organisations. Therefore, also the consent requirement has formed its distinct identity over time and should not be overly emphasised due to the focus of the current legal research.

Accessing location data transmitted by the pets' electronic collars is a modern form of data processing. In this context, the app developer should ensure that the relevant locating infrastructures are robust and that the data transfers between the electronic collars and the operating mobile devices are confidential. Subsequently, the most noteworthy privacy risk connected to this kind of precise locating is the possibility of the indirect location data connections. A pet's location automatically connects to the location of multiple individuals. To avoid the illegal processing of personal data, the app developer should effectively implement the data minimisation principle. This

[295] *Brownsword* 2004, p. 224.
[296] *Aukia* 2018, p. 11.

implementation should be objectively verifiable, meaning that unlawful profiling and other similar data processing are adequately excluded. In doing so, the app developer does not need to acquire consents from all individuals whose personal data is indirectly accessed.

Due to the above specified characteristics of pet monitoring, the most important data protection obligation to demonstrate lawful data processing within the app is not the consent requirement. If consent is considered the sole sufficient basis to protect the fundamental rights and freedoms of the end users, data protection is not comprehensively implemented to the app developer's data protection practices. In doing so, consent can be over-valued in multiple ways. For example, if the app presents excessive information notices to the end users to fulfil the informational requirement for valid consent, it simultaneously disregards their lack of knowledge and weaker bargaining position.[297] In addition, consent can be over-valued by targeting children in the context of the information society service without ensuring that the minors understand all fundamental aspects of the data processing. Accessing special categories of personal data without explicit consents of the end users and without clearly informing the end users on the risks associated with the sensitive data collection also qualifies as over-valuation.

In order the address the problem of consent over-valuation, two data protection obligations can be argued to be more fundamental to the app developer than the consent requirement. These obligations are the implementation of the basic data protection principles and sufficient record-keeping. In the Regulation, it is required that records are kept, among others, of all acquired consents, information notices relating to the consent acquisition, and sufficient security measures. Most importantly, the records should verify that the basic data protection principles are appropriately implemented to the data processing practices of the app developer. Conclusively, the implementation of the principles and record-keeping are overall concepts which reflect data protection comprehensively, not only within one specific aspect. In this regard, the app developer faces the challenge that record-keeping often requires extensive economic and technological resources. In order to address this problem, the Regulation does not set any unequivocal standard which would adequately specify the extent and accuracy of

[297] *Beyleveld and Brownsword* 2007, p. 154.
Bräutigam 2012, p. 426.

required record-keeping. Nevertheless, the app developer competing in consumer business for data collection should at least manage the record-keeping obligation more comprehensively than a data controller engaging in traditional industry and processing only employee related data.[298]

Throughout the application of the Directive and during the transitional period of the Regulation, the Working Party played an important role. It managed to adopt various Opinions addressing specific areas of data protection and to clarify multiple legal obligations imposed on the data controllers. As highly relevant in relation to the app developer, the Working Party recommended that in order to verify a specific consent and its extent, the data controller operating in the online environment should retain information on the session in which the consent was expressed. In addition, it should record the documentation of the consent workflow and a copy of the information that was presented to the specific data subject.[299] In the era of the Regulation, it will be fundamental that the Board effectively continues the work of the Working Party. It should further specify how the data protection framework limits the operations of online companies. In detail, the Board should specify the practical implications of the consent requirement as well as adopt clear standards for required record-keeping. In this regard, the Board should clarify the consent requirement in relation to children[300] and special categories of personal data.

4.2. Redefining data protection

"*The infallibility of the "total memory" of the Internet contrasts with the limits of human memory. Now memory can be the one of rancor, vengeance, or belittlement. Thanks to its "eternity effect", the Internet preserves bad memories, past errors, writings, photos, or videos which we would like to deny later.*"
– EU Publication. *Cécile de Terwangne*. The Right to be Forgotten and the Informational Autonomy in the Digital Environment.

The right to be forgotten and the right to data portability are new concepts which were introduced to the data protection framework in the Regulation. Together they limit the

[298] *Aukia* 2018, p. 12.
[299] Guidelines of the Working Party on Consent under Regulation 2016/679, p. 20.
[300] For example, *Koski* has addressed this problem in her Article (2017, p. 58 – 61).

online retention periods and the unilaterally beneficial relationships relating to the collection and storage of personal data. Despite the practical difficulties in implementing the rights, the app developer is responsible for demonstrating that it appropriately complies with them. In addition, it is responsible for all data processing conducted by the data processors under its control or by other relevant third parties. On the other hand, both the right to be forgotten and the right to data portability significantly affect the economic value of personal data. In the era of the Regulation, location data may not be held as an exclusive economic asset. The end users need to be provided with the factual possibility to personally engage in the modern personal data economy. In other words, the Regulation started a new era of data protection.

After the Regulation was first introduced, the upgraded level of data protection caused vast concern in the corporate world. Private enterprises were particularly worried that the Regulation is too complex and requires extensive implementation resources.[301] The main downside of the stricter rules within the EU was argued to be the negative effect on the competitiveness of the enterprises subject to the rules. According to these arguments, this negative effect is reflected both in the private corporate acquisition processes as well as in service development and innovation possibilities. The enterprises outside the EU have the advantage of processing personal data in a way which in the EU is not lawful. Therefore, the future amendments to the level of data protection should be managed in international organisations or in other international contexts, not in regional administration. The Internet is global and so should be data protection.[302]

As a counter-argument to the concerns in the corporate world, data protection can be argued to have reached an inclusive form. In the modern personal data economy, the data subjects can independently take part in each transaction including their personal information. For them, personal data has become a hybrid legal concept which constantly adapts itself to specific trading situations. If necessary, personal data is defined as property of the data subjects.

Due to the developments in the data protection framework, the inclusive standpoint provides the data subjects with better possibilities to be informed on specific data processing. In addition, the developments strive at preventing negative effects of data

[301] *Kremer* 2016, p. 136.
[302] *Aukia* 2018, p. 13.

breaches (disruption in business, damage to reputation). It should be always ensured that the data subjects know which risks they take when they provide consent to specific data processing. Finally, the inclusive data protection practices contribute to the removal of the gap between the data controllers and the data subjects. In doing so, the enhanced data protection practices in the EU can fundamentally lead to an advantage in competition in relation to the enterprises outside the EU.

In practice, the inclusive from of data protection is well reflected in a corporate acquisition process. In this context, the app developer should adequately limit the publication of location data by the virtue of data protection.[303] The identifiable pets' movement patterns should be transferred to the buyer granularly during the transaction, and the individual disclosures should always have a valid legal basis. Depending on the chosen deal structure, the end users should be provided with sufficient information and the right to opt-out, or be asked to provide new opt-in consents. In addition, the deal execution should be inclusive, and where possible taking account of the confidentiality of the deal, transparent in relation to the end users. Subsequently, prudently conducted data transfers within a corporate acquisition process increase the economic value of the transferred personal data.

[303] *Sartor* 2014, p. 2.