THE PANOPTICON OF COMFORT: RECONCEPTUALISING DATA PRIVACY IN THE SMART HOME ERA

Maja Mlakar, mag. iur. [*]
Izr. prof. dr. Nataša Samec Berghaus [**]

UDK: 342.737/.738:004.7/.8(4)EU
341.231.14:004.7/.8
DOI: 10.3935/zpfz.76.2.2
Pregledni znanstveni rad
Primljeno: rujan 2025.

The article examines how smart-home technologies turn the home into a data-intensive environment in which comfort, security and automation depend on continuous data processing. It argues that GDPR application remains uncertain, especially regarding personal data, controllership among homeowners, device providers and cloud-service providers, and the household exemption. Corporate and cloud-based processing therefore require stronger transparency and accountability, while narrowly tailored domestic security measures should not be equated with large-scale surveillance. Self-protection, particularly to deter crime or preserve evidence concerning property and possession, should be recognised as a weighty legitimate interest, subject to least-intrusive safeguards protecting third parties.

Key words: smart home; GDPR; consent; self-protection; controllership; household exemption

1. SMART HOME: SUBTLE GENERATOR OF BIG DATA

The technology-mediated architecture of the smart home channels an individual's reasonably expected privacy, which is rooted in the vulnerability of

[*] Maja Mlakar, LL. M., Ph. D. student, University of Maribor, Faculty of Law, Mladinska ul. 9, 2000 Maribor, Slovenia; maja.mlakar1@student.um.si; ORCID ID: orcid.org/0009-0000-9730-5676

[**] Nataša Samec Berghaus, Ph. D., Associate Professor, University of Maribor, Faculty of Law, Mladinska ul. 9, 2000 Maribor, Slovenia; natasa.samecberghaus@um.si; ORCID ID: orcid.org/0009-0001-2634-8238

domestic intimacy, into the boundless realm of the global digital cloud and its associated big data ecosystems. The smart home is premised on the integration of interactive technologies, externally manifested primarily through digital sensors and communication devices engineered to anticipate, interpret and respond to user needs – thereby generating a continuous flow of personal data while embedding data collection practices and algorithmic decision-making processes into the private sphere. The ubiquitous, often imperceptible collection of personal data embedded in Internet of Things (IoT) devices undermines the effectiveness of established data protection frameworks, offering in return an illusory sense of comfort, security and cost or energy efficiency.[1]

In the digital era, personal data have emerged as a critical asset, functioning concurrently as currency and as the fundamental resource underpinning economic expansion. Digitized data function as a multifaceted legal and strategic asset, carrying substantial political and economic implications. Within the private sector, they serve predominantly as a source of commercial profit, whereas for state actors, they enable the pursuit and enforcement of interests across multiple dimensions of national security.[2]

The article's research narrative is dedicated to assessing the practical viability of effectively enforcing core data protection principles within the smart home environment, with particular emphasis on the scope of data collection and the lawfulness and transparency of processing activities in the broader context of big data analytics. It further compares users' minimally intrusive security monitoring with third-party privacy through a proportionality lens.

The argument developed herein proceeds from the premise that technological development, particularly in the realm of IoT devices within the smart home, is not neutral but profoundly reshapes the legal relationships among involved actors and significantly impacts the realization of various dimensions of the fundamental right to privacy. Conceived as a dynamic and context dependent concept, privacy demands continuous adaptation of the legal framework to the circumstances in which it is exercised. It faces a novel and complex form of vulnerability, arising not only from external threats but also from the very infrastructural design of the home itself.

---

1 See Bakar, A. A.; Yussof, S.; Ghapar, A. A.; Sameon, S. S.; Jørgensen, B. N., *A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations*, Energies, *vol.* 17, *no.* 5, 2024, p. 3 and Ehrenberg, N.; Harviainen, J. T.; Suominen, J., *Towards Panopticons of Convenience: Power in the Nordic Smart Home Assemblage*, Proceedings of the 26th International Academic Mindtrek Conference, Association for Computing Machinery, New York, 2023, p. 258.

2 See Dowd, R., *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*, Palgrave Macmillan, Cham, 2022, p. 249.

A clear legal definition of the attribute of "smartness" as applied to the concept of the home remains absent. Building upon a range of technical analyses and definitions widely recognized in the literature[3], this article adopts the following working definition to facilitate a focused examination of the pertinent legal issues: "A smart home constitutes a data-intensive living environment grounded in the pervasive integration of IoT devices, with the aim of enabling automation, operational optimization and user-centric control." Beyond comfort and efficiency, security is an inherent telos of the smart home: occupants reasonably expect to deter intrusion, document boundary encroachment, and protect persons and property. IoT devices function through the continuous interconnection of physical sensors with cloud based computational infrastructure, forming a seamless data ecosystem. Environmental data are systematically captured, aggregated with pre-existing datasets in the cloud and processed as an integrated whole. As the volume, variety, and granularity of data inputs increase, the system's analytical capacity is correspondingly amplified, enabling increasingly personalized, predictive, and context sensitive responses within the environment.[4] The reintegration of detected user patterns and preferences into the underlying system contributes to increased service efficiency and a higher degree of personalisation. However, it also raises the risk of invasive profiling that is understood as the derivation of detailed lifestyle insights about individuals based on the analysis and aggregation of data collected through continuous monitoring within the smart home environment.[5] Comparative reviews[6] and classic accounts consistently list safety/security among the core purposes and benefits of smart-home systems (e.g., intrusion detection, smart locks, alarm

[3] See Marikyan, D.; Papagiannidis, S.; Alamanos, E., *A systematic review of the smart home literature: A user perspective*, Technological Forecasting and Social Change, *vol.* 138, 2019, pp. 139 – 154; Ehrenberg, N., *Smart Home Technologies: Convenience and Control*, in: Rousi, R.; von Koskull, C.; Roto, V. (eds.), *Humane Autonomous Technology*, Palgrave Macmillan, Cham, 2024, pp. 182 – 183; Aldrich, F. K., *Smart Homes: Past, Present and Future*, in: Harper, R. (ed.), *Inside the Smart Home*, Springer, London, 2003; Gram-Hanssen, K.; Darby, S. J., *»Home is where the smart is«? Evaluating smart home research and approaches against the concept of home*, Energy Research & Social Science, *vol.* 37, 2018, pp. 96 – 97.

[4] See Bastos, D.; Giubilo, F.; Shackleton, M.; El-Mousa, F., *GDPR Privacy Implications for the Internet of Things*, 4th Annual IoT Security Foundation Conference, *vol.* 4, 2018, p. 2.

[5] See Bakar *et al.*, *op. cit.* (fn. 1), p. 9.

[6] See Marikyan, Papagiannidis, Alamanos, *op. cit.* (fn. 3); Gram-Hanssen, Darby, *op. cit.* (fn. 3); Hargreaves, T.; Hauxwell-Baldwin, R., *Benefits and risks of smart home technologies*, Energy Policy, vol. 103, 2017, pp. 72 – 83.

sensors and remote monitoring), alongside automation and optimisation. Empirical syntheses also show that users expect smart homes to deter break-ins, enable incident documentation and protect persons and property, not only to streamline routines. Socio-technical work on the meaning of home likewise treats the dwelling as a place for security and control, which smart-home infrastructures reconfigure rather than remove. In EU law[7], this security telos is acknowledged where the protection of property, health and life is recognised as a legitimate interest in household video-surveillance; guidance[8] further requires a necessity-and-proportionality assessment rather than categorical exclusion.

2. PRIVACY AS THE DOCTRINAL PERIMETER OF PERSONAL DATA PROTECTION

The concept of privacy rests on the assumption that individuals are entitled to a protected domain of autonomous development, free interaction and uninhibited conduct, insulated from unwarranted interference by third parties. Integral to this sphere is the right to exercise meaningful control over one's personal data.[9]

Solove, one of the world's leading experts in privacy and data security law, characterizes privacy as a concept in disarray. It represents a broad, multifaceted value encompassing freedom of thought, bodily autonomy, solitude within one's home, control over personal data, protection from surveillance, and the safeguarding of one's reputation.[10]

Informational or data privacy operates as a supplementary layer and arguably a foundational prerequisite for the effective protection of other modalities of privacy, by protecting information pertaining to various aspects of an individual's life.[11] It explicitly safeguards values that transcend the traditional bounds

---

7 See C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428.

8 See European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 2020.

9 See La Rue, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40, UN Human Rights Council, Geneva, 2013, para. 22.

10 See Solove, D. J., *Understanding privacy*, Harvard university press, London, 2008, pp. 1 – 2.

11 See Koops, B. J.; Newell, B. C.; Timan, T.; Škorvánek, I.; Chokrevski, T.; Galič, M., *A Typology of Privacy*, University of Pennsylvania Journal of International Law, *vol.* 38, no. 2, 2017, pp. 554 – 555.

of the right to privacy, chief among them the requirements of fair processing, consent or legitimacy.[12] Within the context of the IoT, it serves as a safeguard for data subjects by guaranteeing their awareness of privacy risks associated with smart devices and services, while ensuring they retain meaningful control over their personal data and its subsequent processing.[13]

The boundless data cloud underpinning the IoT is among the most compelling illustrations of how contemporary information technology reconfigures traditionally delineated legal boundaries of jurisdiction between individual states, the European Union and the broader international legal order.

The incursion of technological algorithms into the intimacy of the home environment symbolically dismantles the traditional boundary between the private and public spheres, rendering the notion of privacy increasingly porous both conceptually and legally. These invisible co-inhabitants construct a digital portrait of the user's daily life, where the contours of intimacy are no longer defined by walls, but by protocols and contractual terms, which are rarely read and even more rarely understood by the user. The home is thus reconfigured into a site of continuous interaction – not only between the individual and the IoT device, but also between the individual and the invisible infrastructure of corporate entities, data flows and algorithmic decision-making. Smart home exemplifies the tension between technological capability and legal permissibility, placing the user in a paradoxical position: ostensibly protected yet simultaneously exposed.

The excessive aggregation and improper use of personal data within the IoT ecosystem may give rise to a surveillance architecture resembling a modern panoptic regime, thereby undermining the normative foundation of the individual's reasonable expectation of privacy within the constitutionally protected domain of the home. Smart home environment gives rise to a panopticon of comfort, whereby individuals acquiesce, whether knowingly or unwittingly, to increased surveillance of their private sphere, in return for the tangible or presumed benefits of convenience and efficiency.[14]

---

[12] See De Hert, P.; Gutwirth, S., *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in: Claes, E.; Duff, A.; Gutwirth, S. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, p. 81.

[13] See Harper, S.; Mehrnezhad, M.; Mace, J.; Groß, T.; Viganò, L., *User Privacy Concerns in Commercial Smart Buildings*, Journal of Computer Security, *vol.* 30, no. 3, 2022, p. 468.

[14] See Ehrenberg, Harviainen, Suominen, *op. cit.* (fn. 1), p. 260.

Theoretical articulation of the panopticon modality within the smart home is vividly exemplified by the 2013 Snowden revelations, which exposed a far-reaching surveillance program granting U.S. intelligence agencies access to the data repositories of major technology corporations, collectively known as GAFA (Google, Apple, Facebook, and Amazon). Unlike the classical panopticon, which operates through a single, centralized observer, this surveillance infrastructure relied on multiple data sources, each functioning as an autonomous "sensor." This decentralized, continuous, and ubiquitous system has been conceptualized as a panspectron – a model in which surveillance is diffused across a broad network of interconnected nodes, starting with personal smart devices embedded in everyday life. Unlike traditional surveillance regimes, the panspectron is both omnipresent and persistent, subtly reconfiguring user behavior through the anticipation of observation. Empirical studies have linked this shift to increasing patterns of self-censorship, reflecting a chilling effect on individual autonomy even within the private confines of the home.[15] The distinctiveness of digital surveillance rests on the horizontal architecture of the digital ecosystem, wherein reciprocal user observation dissolves the boundary between observer and observed.[16]

A significant risk also stems from the practice of so-called predictive privacy, which entails algorithmic data mining to infer new information through the cross-correlation analysis of existing Big Data. This phenomenon exemplifies the predominance of surveillance capitalism, driven by market-oriented mechanisms that seek to exploit the behavioral surplus – data generated from user behavior beyond the scope of original consent or necessity.[17]

---

[15] See Laudrain, A., *Smart-city Technologies, Government Surveillance and Privacy: Assessing the Potential for Chilling Effects and Existing Safeguards in the ECHR*, Leiden Law School Working Papers Series, 2019, p. 10.

[16] See Olsson, E.; Öhman, C., *The Quantum Panopticon: A Theory of Surveillance for the Quantum Era*, Minds and Machines, *vol.* 35, 2025, p. 9.

[17] See Orlowski, A.; Loh, W., *Data autonomy and privacy in the smart home: the case for a privacy smart home meta-assistant*, AI & Soc, *vol*. 40, 2025, pp. 4172 – 4173 and Pathmabandu, C.; Grundy, J.; Baruwal Chhetri, M.; Baig, Z., *Privacy for IoT: Informed consent management in Smart Buildings*, Future Generation Computer Systems, *vol.* 145, 2023, p. 370.

3. THE GENERAL DATA PROTECTION REGULATION AS A PILLAR OF TRANSNATIONAL DATA PROTECTION FRAMEWORK

EU law obliges Member States to adhere to the mechanisms established under the General Data Protection Regulation (GDPR)[18], including in the context of the smart home. The GDPR lays down general principles and obligations applicable to the processing of personal data, while neither its recitals nor its substantive provisions specifically address the technological and operational particularities inherent in data processing conducted within IoT ecosystems.[19] Consequently, the GDPR provides only limited guidance regarding the practical application of its requirements within smart home environments, where interconnected IoT devices constitute the core infrastructure for continuous and often pervasive processing of personal data. This lack of regulatory specificity may give rise to interpretative ambiguities and compliance challenges, particularly with respect to the principles of transparency and lawfulness, the validity of consent, the allocation of controllership and liability among multiple actors involved in processing operations, and the effective exercise of data subject rights.

This gives rise to a critical dilemma whether the GDPR's broad scope reflects a deliberate legislative restraint, or whether the current legal framework fails to ensure the highest level of protection for data subjects. The latter concern encompasses both the incomplete realization of the GDPR's foundational principles and the potential inadequacy of specific safeguards such as the right to meaningful information and effective limitations on profiling. The GDPR is frequently regarded as the *de facto* "gold standard" in the field of data protection law, with numerous jurisdictions across the globe, driven by the so-called Brussels Effect, adopting or adapting their domestic legislation in line with its core principles.[20]

---

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1 – 88.

[19] While the GDPR, by virtue of its nature as a regulation, is directly applicable across member states, it nevertheless leaves scope in at least fifty distinct areas for national legislatures to regulate differently through their own data protection laws. In addition, the potential for divergent interpretation and enforcement among member states further contributes to legal fragmentation within the EU. See DLA Piper, *Data Protection Laws of the World – Croatia*, 2025, available at: https://www.dlapiperdataprotection.com/?t=law&c=HR, p. 8.

[20] See Diamantopoulou, V.; Lambrinoudakis, C.; King, J.; Gritzalis, S., *EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era*, in: Knijnenburg, B.P.;

The material scope of the GDPR encompasses personal data, which are defined as any information relating to an identified or identifiable natural person, whether directly or indirectly identifiable.[21] Special categories of personal data are explicitly defined and subject to stricter regulation. These include biometric data, which refer to unique biological attributes, physiological characteristics, or reproducible behavioural patterns specific to an individual. Typical examples within smart home environments encompass fingerprints, retinal patterns, facial geometry and voice characteristics, as well as deeply ingrained behavioural traits such as gait, speech cadence, and distinctive keystroke dynamics.[22] Biometric access or presence systems in smart homes are subject to additional conditions imposed by Member States. In Slovenia, biometric data processing in the private sector is permissible only when strictly necessary for specified purposes (e.g., protection of persons or property) and – crucially – requires prior approval from the Information Commissioner before deployment.[23] In Croatia, biometric data processing by both public and private entities is limited to cases explicitly defined by law and deemed necessary for the protection of individuals, property, classified information, or professional secrets. For private services, secure user identification may only be based on explicit consent, and employers must provide a non-biometric alternative for attendance tracking.[24] German authorities apply Article 9 of the GDPR and have published a national *Positionspapier zur biometrischen Analyse*[25], cautioning against the routine use of biometric systems by private entities while emphasizing the principles of necessity and proportionality. Collectively, these national regulations affirm that biometric deployments within these jurisdictions are exceptional rather than the default.

Page, X.; Wisniewski, P.; Lipford, H. R.; Proferes, N.; Romano, J. (eds.), *Modern Socio-Technical Perspectives on Privacy*, Springer, Cham, 2022, p. 428 and Schwartz, P. M., *Global Data Privacy: The EU Way*, New York University Law Review, *vol.* 94, 2019, p. 778.

21 Art. 4(1) GDPR.

22 See Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 17 WP 136, 2007, p. 8.

23 See Art. 52 and 83 Personal Data Protection Act (ZVOP-2), Zakon o varstvu osebnih podatkov, Uradni list RS, št. 163/22 in 40/25 – ZInfV-1; Information Commissioner of the Republic of Slovenia, *Application for biometric measures*; Information Commissioner of the Republic of Slovenia, *Smernice glede biometrije po ZVOP-2*, 2023.

24 See Zakon o provedbi Opće uredbe o zaštiti podataka (Narodne novine, No 42/2018), Art. 21-24; DLA Piper, *Data Protection Laws of the World – Croatia*, 2025, p. 17.

25 See Datenschutzkonferenz (DSK), *Positionspapier zur biometrischen Analyse*, 2019.

The EU legislator has deliberately assigned a broad interpretation to the notion of personal data[26], reflecting an intent to capture a wide spectrum of information that, by its content, purpose, or effect, relates to an identified or identifiable individual. The broad standards for qualifying information as personal data ensure an expansive material scope, encompassing not only data that directly identifies an individual, but more broadly any information relating to a natural person who is identified or identifiable.[27] European data protection law risks evolving into a 'law of everything'; a normative framework that purports to guarantee the highest standard of legal protection across all contexts, yet proves unworkable in practice.[28] Informational inflation erodes the principle of proportionate and purpose-specific data protection, effectively diminishing the value of the right at the very juncture when its vigorous protection is most warranted. This is particularly significant in the context of smart home ecosystems, where interconnected IoT devices continuously collect and aggregate large volumes of data relating to the same individual across multiple aspects of an individual's behaviour and habits, thereby increasing the likelihood that seemingly non-identifying information may easily constitute personal data when combined with other available data. It should nevertheless be recognised that not every interference with an individual's privacy interests necessarily involves personal data within the meaning of the GDPR, for example where information concerning third persons does not permit their identification.

The fundamental principles governing the processing of personal data as mandated by the GDPR require that such data be processed lawfully, fairly, and transparently, ensuring accuracy and confidentiality. Processing must be confined to the minimum necessary scope, conducted exclusively for specified, explicit, and legitimate purposes, subject to strict storage limitations, and accompanied by comprehensive accountability obligations imposed on the

---

[26] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier /.../ to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. See Art. 4(1) GDPR.

[27] See Case C-434/16, *Nowak*, ECLI:EU:C:2017:994, paras 34-35 and Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, para. 26. Hoofnagle, C. J.; Van der Sloot, B.; Zuiderveen Borgesius, F., *The European Union General Data Protection Regulation: What It Is And What It Means*, Information & Communications Technology Law, *vol.* 28, no. 1, 2019, p. 72.

[28] See Purtova, N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law,* Law, Innovation and Technology, *vol.* 10, no. 1, 2018, p. 42.

data controller.[29] The comprehensive data protection framework experiences a progressive decline in effectiveness within the smart home ecosystem, whereby deficiencies arising at one stage of personal data processing tend to trigger further compliance and enforcement challenges at subsequent stages. This cascading effect is primarily driven by the extensive technological capabilities of IoT devices, which enable continuous, automated, and often imperceptible collection, transmission, and aggregation of personal data across interconnected platforms and services. Consequently, the interconnected and pervasive nature of smart home IoT infrastructures may progressively undermine both the practical effectiveness and enforceability of GDPR safeguards.

4. LEGAL GROUNDS FOR PROCESSING PERSONAL DATA: NAVIGATING PRACTICALITIES

The GDPR establishes six equivalent legal bases for the lawful processing of personal data.[30] The processing of personal data within smart home environments is predominantly grounded in the user's consent. The ethics of consent are rooted in the principle of individual autonomy and represent the cornerstone of informational self-determination in the context of disclosing personal data. In practice, however, smart home users often possess only a limited understanding of the scope of data collection and the potential implications it may entail.[31] Nonetheless, this legal basis proves increasingly problematic in the era of big data, as it remains valid only for predetermined and specific purposes. Yet one of the core characteristics of big data is its inherently unpredictable applications, which often renders consent, within the meaning of the GDPR, ineffective and conceptually diminished.[32]

The data subject's consent refers to any freely given, specific, informed and unambiguous expression of will by which the individual, through a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to them.[33] In numerous instances of big data processing within smart home environments, it is difficult, particularly for users, and even more so for affected third parties, to fully comprehend the scope, mechanisms and

[29] See Recital 39 in relation to Art. 5 GDPR.

[30] See Art. 6 GDPR.

[31] See Orlowski, Loh, *op. cit.* (fn. 17), p. 6.

[32] See Koolen, C., *Transparency and consent in data-driven smart environments*, European Data Protection Law Review, *vol.* 7, no. 2, 2021, p. 176.

[33] See Art. 4(11) GDPR.

implications of such processing. Moreover, the purposes of data processing are frequently defined in broad and vague terms, further obscuring the legitimate interests pursued by controllers. The functioning of IoT devices is generally designed around unobtrusive, nearly imperceptible interactions that minimize the cognitive burden on users. However, this design often, intentionally or otherwise, diminishes users' awareness regarding the collection and use of their data. A particularly concerning practice is the deployment of so-called dark patterns, which subtly steer users toward configuration choices that disproportionately serve the interests of the data controller.[34] The requirement of free and informed consent mandates that data subjects possess a genuine ability to choose and exercise control without facing adverse consequences if they refuse or withdraw their consent. Consent is considered non-voluntary when it is tied to conditions that the individual cannot reject or revoke without experiencing detriment or harm. Where consent to the proposed privacy terms is the sole condition for access to a device, effectively reducing the user's options to a »take-it-or-leave-it« scenario, the dimension of free will is seriously compromised, if not entirely nullified. Such practices are increasingly driven by the rise of the data economy and the entrenchment of surveillance capitalism as a dominant paradigm.[35] Likewise, any consent given within the smart home environment is considered involuntary and therefore invalid where IoT devices, notwithstanding any prior notification, condition access to a service on the user's authorization to process personal data beyond what is strictly necessary for ensuring the device's core functionality. If the user is not provided with a genuine option to refuse the processing of data for additional, nonessential purposes without being excluded from service use, such consent cannot be regarded as freely given. A strong presumption applies that consent to the processing of unnecessary personal data does not constitute valid consent, let alone a lawful substitute in exchange for

[34] See Orlowski, Loh, *op. cit.* (fn. 17), pp. 6 – 7.

[35] For example, during the initial setup of an IoT device within a smart home, the user configures its basic functions. At this stage, the system requests consent for data collection through the device's sensors. Not all of this data may be necessary for the fundamental operation of the device; rather, it may be used by the controller to analyze user habits for the purposes of service improvement or marketing. If the user later withdraws consent for data collection, they may find that certain device functions become disabled or severely limited. This constitutes a case of detriment as outlined in Recital 42 of the GDPR, since the consent was linked to negative consequences upon its withdrawal. Such consent cannot be considered freely given and is therefore invalid. See Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, 17 WP 259, 2018, p. 11.

access to the service.[36] The controller is required to obtain separate consent for each distinct purpose of data processing. Each individual consent request must be accompanied by precise information regarding the types of personal data to be collected for that particular purpose.[37]

Studies have identified a persistent tension between concerns over excessive disclosure of personal data and the continued, unchanged use of such devices; a phenomenon commonly referred to as the Personalisation–Privacy Paradox in the IoT context.[38]

Collection of personal data on the basis of valid consent, conceived in its fullest normative scope, remains the exception rather than the rule within the smart home environment. In contexts where informed consent is implausible, such as instances of covert data collection or when artificial intelligence systems derive additional user-specific inferences, the fundamental right to informational self-determination is undermined.[39]

Less conventional and infrequently relied upon legal basis for data processing in the smart home environment is the performance of a contract to which the data subject is a party. This ground is particularly relevant in situations where the processing of personal data is directly necessary for the fulfilment of contractual obligations agreed between the user and the service provider.[40] The provision is interpreted narrowly and does not encompass cases where the processing is not genuinely necessary for the performance of the contract but would instead be unilaterally imposed by the controller on the data subject.[41]

The mere inclusion of certain data processing activities in a contract does not automatically establish that such processing is necessary for its execution. Contract performance is not a suitable legal basis for profiling a user's habits. Even if secondary purposes of processing are discreetly mentioned in the fine print of the contract, this alone does not demonstrate their necessity for fulfilling

---

36 See Article 29 Data Protection Working Party, *op. cit.* (fn. 35), p. 8.

37 See Article 29 Data Protection Working Party, *op. cit.* (fn. 35), p. 12.

38 See Pathmabandu *et al.*, *op. cit.* (fn. 17), p. 369.

39 See Orlowski, Loh, *op. cit.* (fn. 17), p. 8.

40 For instance, a contract established between the user and the provider of smart lighting control devices may legitimize the controller's collection of data concerning lighting settings, as such data are directly pertinent to the performance of the contractual obligation to deliver lighting adjustment services tailored to the user's preferences.

41 Article 29 Data Protection Working Party, *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 844 WP 217, 2014, p. 17.

the contractual obligations. Crucial to this assessment is a sufficiently specific definition of the processing purposes, which allows for a proper evaluation of their necessity in relation to contract performance.[42]

The legitimate interests legal basis rests upon a balancing exercise between the legitimate interests pursued by the data controller and the fundamental rights and freedoms of the data subject, which may override those interests. The legitimate interest must be real and present, corresponding to the controller's current activities or reasonably anticipated benefits in the near future. Vague or speculative interests are insufficient to satisfy this requirement. The notion of legitimate interest encompasses a broad spectrum of interests, ranging from trivial to essential and from the clearly defined to the more contentious. A more restrictive approach is adopted during the balancing phase, where such interests are weighed against the fundamental rights and freedoms of the data subjects, accompanied by a detailed and context-sensitive substantive analysis.[43] The collection and processing of personal data for the purpose of ensuring long-term management of limited resources, such as electricity and water, may represent a legitimate and compelling interest on the part of data controllers.

5. PURPOSE LIMITATION IN THE AGE OF BIG DATA: DRAWING THE LINE IN A BORDERLESS ENVIRONMENT

The principle of purpose limitation serves as a protective safeguard against the gradual expansion or blurring of the purposes for processing personal data beyond those for which the data subject originally consented; a phenomenon commonly referred to as 'function creep'.[44]

It encompasses both the definition of the purpose and the assessment of the compatibility of any further use of data. The controller must determine the purposes of processing prior to, or at the latest upon, the commencement of personal data collection, and must duly inform the data subject accordingly. The purposes must be lawful, clearly defined, and sufficiently specific to enable the individual to reasonably foresee the consequences of the processing. Broad or vague purposes are not permissible.[45] Broadly defined purposes may lead to excessive data collection that exceeds the actual necessities of the specific pro-

[42] Article 29 Data Protection Working Party, *op. cit.* (fn. 41), p. 17.

[43] See Article 29 Data Protection Working Party, *op. cit.* (fn. 41), p. 24.

[44] See Article 29 Data Protection Working Party, *op. cit.* (fn. 35), p. 12.

[45] For instance, simply stating that video surveillance is conducted for the purpose of 'ensuring security' does not satisfy the requirement of a sufficiently specific

cessing activity. Data controllers must be able to clearly articulate and justify the necessity of collecting and storing personal data.[46] The extrapolation of patterns based on the initial dataset, originally collected for specified primary purposes, can, when combined with the machine learning capabilities of IoT devices, lead to inferences about new data, effectively giving rise to new purposes for data collection. This process also carries the inherent risk of erroneous or misleading inferences. In addition, a substantial volume of the data collected within smart home environments constitutes sensitive personal data. IoT devices are frequently networked with third parties, many of whom are engaged in commercial partnerships with additional entities. This complex web of interconnections significantly heightens the risk of unauthorized dissemination of personal data and may result in unforeseen consequences for end users. GDPR establishes the purpose limitation principle, pursuant to which personal data must be collected for specified, explicit, and legitimate purposes and may not subsequently be processed in a manner incompatible with those purposes. Nevertheless, certain forms of further processing may be recognised as compatible with the original purpose of collection, particularly where such processing is carried out for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.[47] In determining whether processing for a secondary purpose is compatible with the purpose for which the personal data were initially collected, the controller is required to take into account, *inter alia*, the relationship between the original and intended purposes of processing, the context in which the personal data were collected, the nature of the personal data, the possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards, including measures such as encryption or pseudonymisation.[48] The extensive aggregation, sharing, and repurposing of personal data across interconnected devices and multiple commercial actors may render the assessment of compatibility particularly complex. Consequently, it may be questioned whether certain forms of secondary processing within smart home ecosystems – especially those involving behavioural profiling, targeted advertising, predictive analytics, or commercial exploitation by third parties – exceed the reasonable expectations of data sub-

purpose. See Kraigher Mišič, K., *Videonadzor*, in: Kraigher Mišič, K. (ed.), *Uvod v varstvo osebnih podatkov*, GV Založba, Ljubljana, 2024, p. 247.

46 See Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17 WP 251 rev.01, 2018, p. 11.

47 See Art. 5(1)(b) GDPR.

48 See Art. 6(4) GDPR.

jects and may therefore be regarded as incompatible with the original purpose of collection, unless supported by a separate legal basis, particularly valid and informed consent.

The inherent flexibility of the purpose limitation principle allows for its interpretation as marking a transition from a logic of prohibition to one of normative guidance. In this context, ensuring that data collection is limited to what is strictly necessary for the specific purpose of processing is often *prima facie* difficult to achieve, as IoT devices tend to gather data in ways that exceed the functional necessities of the system.

6. TRANSPARENCY OF DATA PROCESSING: THE TANGIBLE INVISIBILITY PARADOX

Transparency entails providing the data subject with access to specific information. The overarching aim of the transparency principle is to level the playing field and address the information asymmetries that frequently exist between data subjects and data controllers, who typically occupy a position of power. By enhancing individuals' awareness and understanding of how their data are processed, the principle of transparency strengthens their position and enables greater control over their personal data. It is fundamental to the realization of informational privacy. It stems from the necessity to establish mechanisms that balance the inherently opaque and potentially biased nature of data collection and processing. The actual degree of user awareness concerning data processing in smart home IoT devices tends to approximate the concept of translucency rather than the ideal of fully targeted transparency. The persistent tension between normative transparency requirements and practical realities is primarily driven by ongoing, complex technological developments, which often hinder a complete understanding of the consequences of data processing. Consequently, users generally retain only a vague or superficial grasp of the scope and nature of these processing activities. Awareness of data processing activities is essential to enable individuals to exercise control, impose restrictions, adjust, or prevent such operations. It could be substantially improved by imposing a clear and emphasized obligation on providers of IoT devices to disclose not only their key functionalities but also the types of embedded sensors and their technical capabilities for data collection. Of particular importance is the precise specification of the categories of personal data collected. Users typically infer data processing solely from the basic characteristics of the device; however, less obvious data types are often collected, which users may not anticipate. However, users in practice often exhibit a degree of indifference, failing to engage with the

extensive information provided, thereby undermining regulatory efforts aimed at protecting them. Some may be discouraged by the technical complexity of such notices, while others may simply lack interest in being informed, focusing instead on the perceived utility and convenience offered by the devices.[49] In the digital environment, data subjects are routinely exposed to a multitude of consent requests, often requiring responses through simple clicks or swipes. As users become increasingly saturated with such prompts, the intended cautionary or protective function of consent mechanisms is significantly eroded. This dynamic fosters a condition of so-called informational ignorance, which poses particular risks for individuals, especially when consent is solicited for actions that, in the absence of such consent, would arguably be unlawful. In this regard, parallels may be drawn with the regulatory approach adopted under the Digital Services Act (DSA)[50], which establishes the concept of "dark patterns", referring to online interface designs or practices that materially distort or impair, whether intentionally or in practice, the ability of recipients of the service to make autonomous and informed choices or decisions.[51] The GDPR therefore imposes a duty on controllers to proactively design and implement effective, accessible, and user-centric mechanisms that facilitate genuine transparency and informed consent.[52]

7. PROFILING: THE DATA-DRIVEN SHAPING OF IDENTITY

Profiling refers to any form of automated processing of personal data that involves the use of such data to evaluate certain personal aspects relating to an individual.[53] This entails the formulation of specific inferences about an individual by extrapolating from the attributes of other persons who are statistically similar, thereby ascribing characteristics to the individual based on group-level correlations. Through the analysis of data in conjunction with other datasets, it becomes possible to uncover patterns and correlations that are not immediately

[49] See Koolen, *op. cit.* (fn. 32), p. 178.

[50] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, pp. 1 – 102.

[51] See Recital 67 and Art. 25 DSA.

[52] See Article 29 Data Protection Working Party, *op. cit.* (fn. 35), p. 18.

[53] The profiling process comprises three distinct stages: the collection of data, the automated analysis of that data to identify correlations and the application of those correlations to individuals in order to infer characteristics of their current or future behaviour. See Article 29 Data Protection Working Party, *op. cit.* (fn. 46), p. 7.

apparent. Particularly concerning is the fact that corporations often pursue specialised interests in data collection and processing that extend beyond what is strictly necessary for the functionality or intended use of a given device.[54] Profiling imparts a personalised dimension to the smart home environment, enabling efficient interactions – seamlessly executed tasks tailored to the user's needs with minimal effort required on their part. To a certain extent, profiling is reasonably necessary to deliver the level of service users have come to expect. There exists a significant risk that special categories of personal data may be constructed through inference, based on information that is not inherently sensitive but acquires such a character when combined with other datasets.[55]

To invoke the restriction on automated individual decision-making, including profiling[56], the relevant activity must produce a significant effect. Yet, individual minor automated decisions based on profiling within the smart home context are typically not regarded as producing tangible harm to the data subject. This prevailing assumption warrants critical scrutiny, as IoT devices, through the accumulation of seemingly inconsequential actions, are in fact reshaping the domestic sphere in profound ways. It is therefore necessary to reassess the appropriateness of requiring a direct causal link between a specific automated decision, the profiling activity, and a harmful consequence. The technological complexity and interconnectedness of smart home ecosystems indicate that adverse impacts on the user's fundamental rights and interests may stem from the cumulative effect of numerous, individually negligible operations.

Ultimately, the question arises whether the data generated by an IoT device through profiling, based on initial personal data and processed by artificial intelligence, can still be regarded as personal data in the material sense under the GDPR. While algorithmic processing may significantly contribute to managing informational complexity, it also introduces a risk of producing fundamentally flawed inferences derived from the available data sets.[57]

---

54 See Koolen, *op. cit.* (fn. 32), p. 176.

55 For instance, a smart refrigerator may collect data on an individual's grocery purchases, which, when analysed alongside information about nutritional content and product quality, can yield inferences about that individual's health status. See Article 29 Data Protection Working Party, *op. cit.* (fn. 46), p. 15.

56 See Art. 22 GDPR.

57 See Koolen, *op. cit.* (fn. 32), p. 176.

8. BETWEEN JOINT CONTROLLERSHIP AND THE HOUSEHOLD EXEMPTION

Within the accountability framework established by the GDPR, the controller[58] occupies a central position in ensuring the lawfulness of personal data processing[59], while joint controllership applies where two or more actors jointly determine the essential purposes and means of processing.[60] In smart home ecosystems, controllership should therefore be mapped functionally rather than formally. Where IoT devices are used locally and exclusively for personal or household purposes, the homeowner will generally fall outside the GDPR's scope under the household exemption. Where monitoring extends beyond the private sphere, for instance by systematically capturing visitors, neighbours or public space, the homeowner may qualify as a controller for that specific processing operation. By contrast, device manufacturers, app providers, cloud platforms and analytics service providers will normally qualify as controllers where they determine the purposes and means of processing for service provision, diagnostics, product improvement, profiling, marketing or data sharing with third parties. They may act as processors only where they process data solely on documented instructions and without independent purposes. Joint controllership may arise only where the homeowner and provider jointly determine essential purposes and means; mere use of a standardised device or service should not, by itself, be treated as sufficient for joint controllership. The scope of the household exemption can therefore be assessed only after the relevant processing operation, controller and data subjects have been identified.[61]

8.1. Balancing Third-Party Privacy and the Right to Self-Protection in the Smart Home

The deployment of surveillance and sensor technologies in smart homes raises a tension between the privacy rights of third parties and the homeowner's interest in self-protection. European data protection law strongly safeguards the privacy of anyone captured by such systems, often restricting private video surveillance

58 See Art. 4(7) GDPR.

59 See Art. 5(2) GDPR.

60 See Art. 26 GDPR.

61 See Chen, J.; Edwards, L.; Urquhart, L.; McAuley, D., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption*, International Data Privacy Law, *vol.* 10, no. 4, 2020, p. 291.

that extends beyond one's own domestic sphere. Under the GDPR's "household exemption", data processing carried out by an individual purely for personal or household activities falls outside the regulation's scope. However, the Court of Justice of the EU in C-212/13, *Ryneš* clarified that this exemption is to be interpreted narrowly: a home security camera directed at public space (such as a sidewalk or a neighbor's entrance) does not qualify as "purely household" processing and therefore triggers full data protection compliance.[62] In that case, a homeowner had installed a CCTV camera on his family home after repeated vandalism and attacks, but because the camera recorded a public footpath and the entrance of a house across the street, the EU Data Protection Directive (precursor to the GDPR) was found to apply in full. The individual was deemed a data controller and was found to have violated data protection law by recording people in public without their consent, failing to inform them, and not registering the processing with authorities. Notably, the CJEU acknowledged the legitimate interest of the homeowner in protecting the life, health, and property of his family, but it held that such interest must be pursued within the confines of data protection requirements. In other words, private safety interests do not categorically override privacy law – they must be balanced within it. Drawing on the case law of the Supreme Court of the Republic of Slovenia, the case law of the Higher Court in Ljubljana emphasises that in cases involving a conflict between coexisting rights within horizontal relationships between formally equal individuals, the permissibility of interference with another's right must be assessed through the doctrine of practical concordance, rather than through the application of the principle of proportionality. The court is required to determine, by means of a careful balancing of the competing rights in light of all the specific circumstances of the individual case, which of the rights must be given precedence in the particular situation, while the remaining rights may be exercised only to the extent that their exercise does not preclude the effective realisation of the competing right.[63]

A critical issue is whether the same level of regulatory stringency – designed for government or large-scale corporate surveillance – should apply when an individual homeowner seeks to protect his or her domicile. Under the letter of current law, once a smart home user's surveillance extends beyond "purely household" context, they indeed assume the full obligations of a data controller, just like a municipality or a business.[64] In principle, the GDPR does not distinguish between a city government using AI cameras and a person installing a smart

[62] ECLI:EU:C:2014:2428.

[63] VSL I Ip 184/2023, 22.02.2023, ECLI:SI:VSLJ:2023:I.IP.184.2023, para. 10.

[64] See Zoltan, M., *At Least 65 Private Individuals Were Fined for GDPR Violations Since 2018*, Privacy Affairs, 2022.

CCTV to watch over the garden fence; both must have a lawful basis, respect data subject rights, and implement safeguards, or else face liability. Yet this formal parity gives rise to palpable inequities and practical difficulties. Private individuals generally lack the legal knowledge and resources to implement measures such as detailed privacy notices to passers-by, rigorous data protection impact assessments, or advanced anonymization techniques. Unlike public authorities, they cannot invoke statutory powers or public interest tasks to justify their surveillance; at best, they must rely on the more limited and case-specific basis of "legitimate interests"[65] to defend the necessity of their monitoring. Member State practice further narrows the scope of the GDPR's "household exemption" for home surveillance. In Slovenia, the DPA explains that a private camera falls within the purely personal/household sphere only if it captures exclusively the owner's premises; once any public space or a neighbour's property is recorded, the individual becomes a controller subject to ZVOP-2[66]/GDPR duties. Video surveillance of multi-apartment buildings containing only private dwellings (former Article of the 76 ZVOP-1[67]) is no longer explicitly regulated, and the provisions of the GDPR apply to its establishment and implementation.[68] Croatia goes further: its GDPR Implementation Act allows monitoring of public areas only by public authorities or entities entrusted with public tasks; private persons may not film streets or other public spaces.[69] Germany, by contrast, regulates the video surveillance of publicly accessible areas in § 4 BDSG: private monitoring is permitted only where necessary to pursue legitimate interests (e.g., protection of property), subject to strict balancing and clear information duties.[70] Taken together, these examples operationalise a narrow construction of the household exemption and set a high compliance bar for private CCTV around the home. This puts homeowners in an uneasy position – expected to

65 See Art. 6(1)(f) GDPR.

66 See Art. 80 ZVOP-2.

67 Zakon o varstvu osebnih podatkov, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 177/20 – ZVOPOKD in 163/22 – ZVOP-2.

68 See Information Commissioner of the Republic of Slovenia, *Establishment of video surveillance (Article 76 ZVOP 2)*. Legitimate interest should be interpreted so as not to impose disproportionate obligations on the controller. The lawful basis for recordings lies in the protection of property, and any additional duties should extend only insofar as necessary to achieve that security objective.

69 See Zakon o provedbi Opće uredbe o zaštiti podataka (Act on the Implementation of the General Data Protection Regulation), Narodne novine, No. 42/2018, Art. 32.

70 § 4 BDSG: »Video surveillance of publicly accessible spaces«, Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

adhere to professional-grade privacy standards even as they act in a personal capacity to secure what are often fundamental rights and interests, like personal safety or property protection. We submit that the current framework strikes an unbalanced allocation of rights, heavily favouring the privacy of potential intruders or third parties while affording insufficient weight to the individual's right to protect oneself and one's home. Accordingly, we argue for a proportionate rebalancing: narrowly tailored domestic security measures should be recognised as a weighty legitimate interest when implemented with light-touch (rather than onerous) safeguards. Incidental capture of a small strip of public space or a neighbour's boundary – unavoidable when monitoring a front door, driveway, or plot boundary – should not disqualify household security from the legitimate-interest analysis; instead, it should trigger a necessity-and-proportionality check calibrated to the realities of home defence.[71]

9. CONCLUSION

The unique convergence of domestic and informational privacy transforms the smart home from an individual's most secure sanctuary into a domain rife with latent risks – subtle yet pervasive threats concealed beneath the veneer of technological convenience.

The foundational principles governing the collection and processing of personal data under the GDPR are intricately interconnected and mutually dependent. Within the complex ecosystem of the smart home, these principles increasingly yield to a corporate oligarchy that exploits technological capabilities to circumvent gaps inherent in (programmatically) designed legislation. Central to the smart home is the user's digital profile, whose integrity stands in inverse relation to the lawfulness of data collection and processing practices. Any violation of the principle of data minimization, which confines data collection strictly to what is necessary for a specified purpose, about which the controller must inform the data subject to enable valid consent, undermines the mechanisms that safeguard an individual's reasonable expectation of privacy in their domestic environment. Consequently, the assumption that the informed smart home user maintains effective control over their personal data is no longer tenable.

[71] Compare Orla Lynskey's analysis of the "privileged" status and strict judicial interpretation of data protection in EU adjudication, and Zdeněk Kühn's critique of extending strict EU data rules to inherently local, household-scale CCTV as alienating and ineffective for ordinary citizens. Lynskey, O., *Complete and Effective Data Protection*, Current Legal Problems, *vol.* 76, no. 1, 2023, pp. 297 – 344; Kühn, Z., *The Ryneš Case and Liability for Invasion of Privacy in the 21st Century*, Croatian Yearbook of European Law & Policy, *vol.* 14, 2018, pp. 241 – 253.

The smart home should therefore not be treated as a legally homogeneous environment. Its data flows must be distinguished according to the actor determining the purposes and means of processing, the identifiability of the persons concerned, and the spatial and functional reach of the processing operation. Purely domestic and locally confined uses may fall within the household exemption, even where they incidentally involve ordinary interactions within the home. By contrast, processing performed by device manufacturers, cloud providers, app operators or analytics partners remains subject to the GDPR whenever those actors independently determine the purposes and means of processing, particularly for profiling, service optimisation, marketing, product development or data sharing. Similarly, homeowners may themselves assume controller responsibilities where monitoring extends beyond the private sphere or systematically affects persons outside the household.

This differentiation is essential for avoiding both under- and over-regulation. On the one hand, the opacity, aggregation and secondary use of smart home data by corporate actors require a more substantive application of transparency, purpose limitation, data minimisation and accountability. On the other hand, narrowly tailored domestic security measures should not be subjected to the same practical burden as large-scale public or commercial surveillance. Self-protection should be recognised as a weighty legitimate interest, but only where the measure is necessary, spatially limited, storage-restricted, transparent where feasible, and designed to minimise the capture of third parties.

The recalibration required by the smart home era is thus twofold: stronger accountability at the corporate and cloud-processing layers, and a more proportionate, context-sensitive application of data protection obligations at the household layer. Only such an approach can preserve the home as a space of privacy and autonomy without denying individuals the ability to protect persons, property and possession through least-intrusive technological means.

BIBLIOGRAPHY

Aldrich, F. K., *Smart Homes: Past, Present and Future*, in: Harper, R. (ed.), *Inside the Smart Home*, Springer, London, 2003, pp. 17 – 39, DOI: 10.1007/1-85233-854-7_2.

Bakar, A. A.; Yussof, S.; Ghapar, A. A.; Sameon, S. S.; Jørgensen, B. N., *A Review of Privacy Concerns in Energy-Efficient Smart Buildings: Risks, Rights, and Regulations*, Energies, *vol.* 17, no. 5, 2024, pp. 1 – 17, DOI: 10.3390/en17050977.

Bastos, D.; Giubilo, F.; Shackleton, M.; El-Mousa, F., *GDPR Privacy Implications for the Internet of Things*, 4th Annual IoT Security Foundation Conference, *vol.* 4, 2018, pp. 1 – 8.

Chen, J.; Edwards, L.; Urquhart, L.; McAuley, D., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption*, International Data Privacy Law, *vol.* 10, no. 4, 2020, pp. 279 – 293, DOI: 10.1093/idpl/ipaa011.

De Hert, P.; Gutwirth, S., *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in: Claes, E.; Duff, A.; Gutwirth, S. (eds.), *Privacy and the criminal law*, Intersentia, Antwerp, Oxford, 2006, pp. 61 – 104, DOI: 10.11117/rdp.v18i100.6200.

Diamantopoulou, V.; Lambrinoudakis, C.; King, J.; Gritzalis, S., *EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era*, in: Knijnenburg, B. P.; Page, X.; Wisniewski, P.; Lipford, H. R.; Proferes, N.; Romano, J. (eds.), *Modern Socio-Technical Perspectives on Privacy*, Springer, Cham, 2022, pp. 427 – 448, DOI: 10.1007/978-3-030-82786-1_18.

Diligenski, A.; Prlja, D.; Cerović, D., *Pravo zaštite podataka GDPR*, Institut za uporedno pravo, Beograd, 2018.

Dowd, R., T*he Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*, Palgrave Macmillan, Cham, 2022, DOI: 10.1007/978-3-030-82969-8.

Ehrenberg, N.; Harviainen, J. T.; Suominen, J., *Towards Panopticons of Convenience: Power in the Nordic Smart Home Assemblage*, in: *Proceedings of the 26th International Academic Mindtrek Conference*, Association for Computing Machinery, New York, 2023, pp. 257 – 266, DOI: 10.1145/3616961.3616962.

Ehrenberg, N., *Smart Home Technologies: Convenience and Control*, in: Rousi, R.; von Koskull, C.; Roto, V. (eds.), *Humane Autonomous Technology*, Palgrave Macmillan, Cham, 2024, pp. 181 – 198, DOI: 10.1007/978-3-031-66528-8_8.

Gram-Hanssen, K.; Darby, S. J., *»Home is where the smart is«? Evaluating smart home research and approaches against the concept of home*, Energy Research & Social Science, *vol.* 37, 2018, pp. 94 – 101, DOI: 10.1016/j.erss.2017.09.037.

Harper, S.; Mehrnezhad, M.; Mace, J.; Groß, T.; Viganò, L., *User Privacy Concerns in Commercial Smart Buildings*, Journal of Computer Security, *vol.* 30, no. 3, 2022, pp. 465 – 497, DOI: 10.3233/JCS-210035.

Hoofnagle, C. J.; Van der Sloot, B.; Zuiderveen Borgesius, F., *The European Union General Data Protection Regulation: What It Is And What It Means*, Information & Communications Technology Law, *vol.* 28, no. 1, 2019, pp. 65 – 98, DOI: 10.1080/13600834.2019.1573501.

Koolen, C., *Transparency and consent in data-driven smart environments*, European Data Protection Law Review, *vol.* 7, no. 2, 2021, pp. 174 – 189, DOI: 10.2139/ssrn.3597736.

Koops, B. J.; Newell, B. C.; Timan, T.; Škorvánek, I.; Chokrevski, T.; Galič, M., *A Typology of Privacy*, University of Pennsylvania Journal of International Law, *vol.* 38, no. 2, 2017, pp. 483 – 575.

Kraigher Mišič, K., *Videonadzor*, in: Kraigher Mišič, K. (ed.), *Uvod v varstvo osebnih podatkov*, GV Založba, Ljubljana, 2024, pp. 246 – 254.

Kühn, Z., *The Ryneš Case and Liability for Invasion of Privacy in the 21st Century*, Croatian Yearbook of European Law & Policy, *vol.* 14, 2018, pp. 241 – 253, DOI: 10.3935/cyelp.14.2018.302.

Laudrain, A., *Smart-city Technologies, Government Surveillance and Privacy: Assessing the Potential for Chilling Effects and Existing Safeguards in the ECHR*, Leiden Law School Working Papers Series, 2019.

Lynskey, O., *Complete and Effective Data Protection*, Current Legal Problems, *vol.* 76, no. 1, 2023, pp. 297 – 344, DOI: 10.1093/clp/cuad009.

Marikyan, D.; Papagiannidis, S.; Alamanos, E., *A systematic review of the smart home literature: A user perspective*, Technological Forecasting and Social Change, *vol.* 138, 2019, pp. 139 – 154, DOI: 10.1016/j.techfore.2018.08.015.

Olsson, E.; Öhman, C., *The Quantum Panopticon: A Theory of Surveillance for the Quantum Era*, Minds and Machines, *vol.* 35, 2025, DOI: 10.1007/s11023-025-09723-2.

Orlowski, A.; Loh, W., *Data autonomy and privacy in the smart home: the case for a privacy smart home meta-assistant*, AI & Soc, *vol.* 40, no. 6, 2025, pp. 4171 – 4184, DOI: 10.1007/s00146-025-02182-4.

Pathmabandu, C.; Grundy, J.; Baruwal Chhetri, M.; Baig, Z., *Privacy for IoT: Informed consent management in Smart Buildings*, Future Generation Computer Systems, *vol.* 145, 2023, pp. 367 – 383, DOI: 10.1016/j.future.2023.03.045.

Purtova, N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law,* Law, Innovation and Technology, *vol.* 10, no. 1, 2018, pp. 40 – 81, DOI: 10.2139/ssrn.3036355.

Schwartz, P. M., *Global Data Privacy: The EU Way*, New York University Law Review, *vol.* 94, 2019, pp. 771 – 818.

Solove, D. J., *Understanding privacy,* Harvard university press, London, 2008.

Zoltan, M., *At Least 65 Private Individuals Were Fined for GDPR Violations Since 2018*, Privacy Affairs, 2022, (https://www.privacyaffairs.com/private-individuals-gdpr/) (20 August 2025).

Wilson, C.; Hargreaves, T.; Hauxwell-Baldwin, R., *Benefits and risks of smart home technologies*, Energy Policy, *vol.* 103, 2017, pp. 72 – 83, DOI: 10.1016/j.enpol.2016.12.047.

SOURCES

Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17 WP 251 rev.01, 2018.

Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, 17 WP 259, 2018.

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 17 WP 136, 2007.

Article 29 Data Protection Working Party, *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 844 WP 217, 2014.

Act on the Implementation of the General Data Protection Regulation (Zakon o provedbi Opće uredbe o zaštiti podataka), Narodne novine, No. 42/2018, https://azop.hr/national-legislation/ (18 August 2025).

Croatian Personal Data Protection Agency, *Act on the Implementation of the General Data Protection Regulation*, https://azop.hr/national-legislation/ (18 August 2025).

Datenschutzkonferenz (DSK), *Positionspapier zur biometrischen Analyse*, 2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf (18 August 2025).

DLA Piper, *Data Protection Laws of the World – Croatia*, 2025.

European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, 2020.

Information Commissioner of the Republic of Slovenia, *Application for biometric measures*, https://www.ip-rs.si/en/data-protection/obligations-of-data-processors/application-for-biometric-measures (18 August 2025).

Information Commissioner of the Republic of Slovenia, *Establishment of video surveillance (Article 76 ZVOP 2)*, https://www.ip-rs.si/en/data-protection/obligations-of-data-processors/establishment-of-video-surveillance (18 August 2025).

Information Commissioner of the Republic of Slovenia, *Smernice glede biometrije po ZVOP-2*, 2023, https://www.ip-rs.si/prirocniki_smernice/Smernice%20glede%20uvedbe%20biometrijskih%20ukrepov_2.0_%20%28ZVOP-2%29.pdf (18 August 2025).

La Rue, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/23/40, UN Human Rights Council, Geneva, 2013.

Sažetak

Maja Mlakar *
Nataša Samec Berghaus **

PANOPTIKON UDOBNOSTI: NOVI POGLED NA PRIVATNOST PODATAKA U ERI PAMETNIH DOMOVA

Članak analizira kako tehnologije pametnoga doma pretvaraju dom u podatkovno intenzivno okruženje u kojem udobnost, sigurnost i automatizacija ovise o kontinuiranoj obradi podataka. Tvrdi se da je primjena GDPR-a i dalje nejasna, osobito u pogledu osobnih podataka, vođenja obrade podataka u odnosu između vlasnika doma, pružatelja uređaja i pružatelja usluga u oblaku te izuzeća za osobne i kućne aktivnosti. Korporativna obrada i obrada u oblaku stoga zahtijevaju strožu transparentnost i odgovornost, dok se usko ciljane sigurnosne mjere u domu ne bi smjele izjednačavati s opsežnim nadzorom. Samozaštitu, osobito radi odvraćanja od kaznenih djela ili očuvanja dokaza glede vlasništva i posjeda, treba priznati kao važan legitiman interes, uz najmanje intruzivne zaštitne mjere za treće osobe.

Ključne riječi: pametni dom; GDPR; pristanak; uloga voditelja obrade; izuzeće za osobne i kućne aktivnosti; samozaštita

* Maja Mlakar, mag. iur., doktorandica Pravnog fakulteta Sveučilišta u Mariboru, Mladinska ul. 9, 2000 Maribor, Slovenija; maja.mlakar1@student.um.si; ORCID ID: orcid.org/0009-0000-9730-5676

** Dr. sc. Nataša Samec Berghaus, izvanredna profesorica Pravnog fakulteta Sveučilišta u Mariboru, Mladinska ul. 9, 2000 Maribor, Slovenija; natasa.samecberghaus@um.si; ORCID ID: orcid.org/0009-0001-2634-8238