Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases

FUTURE OF PRIVACY FORUM

NYMITY
innovating compliance

Processing Personal Data on the Basis of Legitimate Interests under the GDPR

PRACTICAL CASES

The Future of Privacy Forum and **Nymity** would like to thank **Gabriela Zanfir-Fortuna** (Policy Counsel, FPF) and **Teresa Troester-Falk** (Chief Global Privacy Strategist, Nymity) for authoring this paper and **Meaghan McCluskey** (Director, Compliance Research, Nymity) principal researcher.

Table of Contents

1. Overview

Legitimate interest has long been one of the primary methods relied on by organizations for processing data for many different types of processing. Other than in the case of public authorities, "legitimate interests", as a basis for lawful processing, is not substantially changed by the General Data Protection Regulation[1] (GDPR). Indeed, Article 7(1)(f) of Directive 95/46[2], as well as Article 6(1)(f) of the GDPR allow processing of personal data on the grounds of legitimate interests of the controller or third-parties.

However, using the "legitimate interests" ground for lawful processing is far more complicated than merely having a legitimate interest to process the personal data at issue. The "balancing exercise" that must be conducted between the interests of the controller or third parties and the rights and freedoms of the data subject is a very important component of lawfully using this ground for processing. Equally important is the "necessity" of processing that data to accomplish that specific interest. But all this sounds theoretical and difficult to grasp in practice, despite guidance that have been issued by European Data Protection Authorities and by other organizations.

The **Future of Privacy Forum** and **NYMITY** collaborated to create this Report and identify specific cases that have been decided at the national level by Data Protection Authorities (DPAs) and Courts from the European Economic Area (EEA), as well as the most relevant cases where the Court of Justice of the European Union interpreted and applied the "legitimate interests" ground. We looked at cases across industries and we compiled them in two lists: one for uses of this ground that were found lawful and one for uses that were found unlawful. All of them contain useful examples of how the "balancing exercise" is conducted in practice, as well as examples of safeguards that were needed to tilt the balance and make the processing lawful. Some of them have short comments at the end of the summary that point out interesting features of the case.

The Report is divided in two parts: "Background" and "Legitimate Interests in Practice". The Background provides brief details of the significance of lawful grounds for processing in general, the relevant legal requirements and the guidance that has been issued by the Article 29 Working Party (WP29) or individual DPAs. It also clarifies that relying on "legitimate interests" instead of "consent" still means that data protection notices must be given to data subjects and that the rights of the data subject, with the exception of portability, still apply.

"Legitimate Interests in Practice" first looks at specific cases from the Court of Justice of the EU. We will see that for instance the outcome of the famous "right to be forgotten case" from 2014 was decisively influenced by how the Court interpreted processing on the "legitimate interests" of the controller, an aspect that is often overlooked when analyzing the *Google Spain* case. The following section summarizes cases where the use of "legitimate interests" was found unlawful, and the last section summarizes cases where the use of "legitimate interests" was found lawful.

We hope this comprehensive Report of concrete cases will be found useful by all industries and will contribute to effective data protection for individuals.

[1] Regulation (EU) 679/2016 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.

[2] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281.

2. Background

2.1 The big picture: Understanding the function of lawful grounds for processing

The principle of lawfulness is fundamental for the right to the protection of personal data, as set out in EU law. Article 8(2) of the Charter of Fundamental Rights of the EU specifies that personal data must be processed "on the basis of the consent of the person concerned or some other legitimate basis laid down by law". The principle of lawfulness is provided for in the General Data Protection Regulation, which requires that personal data must be "processed lawfully, fairly and in a transparent manner in relation to the data subject"[3].

As explained in one of the recitals of the GDPR, "in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation (…)"[4].

According to the Regulation, the condition of lawfulness is fulfilled only when at least one of the six legitimate grounds for processing detailed in Articles 6 applies:

1. **Consent:** The data subject has given consent to the processing of his or her personal data for one or more specific purposes[5].

2. **Performance of a contract:** Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract[6].

3. **Legal obligation:** Processing is necessary for compliance with a legal obligation to which the controller is subject.

4. **Vital interests:** Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

5. **Task in the public interest:** 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;

6. **Legitimate interests:** Processing is necessary for the purposes of the legitimate interests 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.

Any processing of personal data must be based on one of these six grounds, with the exception of processing special categories of data (sensitive data), which enjoys additional, special rules.

[3] Article 5(1)(a) GDPR.
[4] Recital 40 GDPR.
[5] Article 6(1)(a) GDPR.
[6] Article 6(1)(b) GDPR.

It is important to note that there is no hierarchy among the legitimate grounds for processing.

The GDPR has specific rules for the lawful grounds of processing special categories of data, under Article 9, which means that whenever one of the special categories of data is processed, the Article 9 rules on permissible uses of sensitive data are applicable. The Article 29 Working Party explained that a controller processing special categories of data may never invoke solely the general grounds for processing, currently under Article 6 GDPR. These rules "will not prevail, but always apply in a cumulative way" with the rules for processing special categories of data[7].

The special categories of data are enumerated in an exhaustive list in Article 9 GDPR:

- data revealing racial or ethnic origin,
- political opinions,
- religious beliefs,
- philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data (for the purpose of uniquely identifying a natural person)
- data concerning health,
- data concerning sex life or sexual orientation.

Processing of these special categories of data is prohibited, as a rule, under the first paragraph of Article 9 GDPR. Their processing is allowed under one of the exceptions provided for by the second paragraph of Article 9:

1. **Consent** : Explicit consent of the data subject;

2. **Employment and social security law**: Carrying out obligations under employment and social security protection law (if authorized by law or by a collective agreement);

3. **Vital interests**: Necessity to protect the vital interests of the data subject or of another person;

4. **Political/religious not-for-profits** : Carried out with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it and that the personal data are not disclosed outside that body without consent;

5. **Data manifestly made public**: Processing relates to personal data which are manifestly made public by the data subject;

6. **Legal claims**: Necessity for establishing, exercise or defense of legal claims;

7. **Substantial public interest:** Necessity for reasons of substantial public interest, on the basis of Union or Member State law;

8. **Medical purposes**: Necessity for the purposes of preventive or occupational medicine, for the assessment of the working capacity of employee, medical diagnosis, the provision of

[7] Article 29 Working Party, "Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46", April 9, 2014, p. 15.

health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

9. **Public health:** Necessity for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law;

10. **Archiving, scientific or historical research:** Necessity for reasons of public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law.

Additionally, Member States may introduce new conditions, including limitations, if they concern processing of genetic data, biometric data or data concerning health[8].

Finally, the GDPR also enshrines a special rule concerning the lawfulness of processing personal data relating to criminal convictions and offences, in Article 10. Processing this type of data on the basis of Article 6(1) must be "carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects". This is relevant for instance in employment contexts, where employers ask prospective employees to provide their criminal record. It looks like excerpts from criminal records will not be able to be used in the employment process on the basis of the consent of prospective employees, unless national laws will allow it and will provide safeguards. Further guidance is needed for the application of Article 10, especially since the recitals do not elaborate on it.

2.2 Processing personal data on the basis of legitimate interests, in the GDPR

According to Article 6(1)(f), processing is lawful if it is "necessary for the purposes of legitimate interests 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". According to the last sentence of Article 6(1)(f), this lawful ground for processing does not apply to processing carried out by public authorities in the performance of their tasks.

Having a closer look at the legal text, there are three elements for this lawful ground for processing to be applicable:

1. **Necessity:** Often overlooked, necessity is the first element that needs to be complied with when relying on legitimate interests as lawful ground for processing. Thus, the personal data being processed must be "necessary" for those legitimate interests to be achieved. This means that any data item that is not directly linked to obtaining, realizing or otherwise accomplishing the legitimate interests pursued is not processed lawfully. Necessity implies the need for a combined, fact-based assessment of the effectiveness of processing that data for the objective pursued and of whether processing that data is less intrusive for the rights of individuals compared to other options for achieving the same goal[9].

[8] Article 9(4) GDPR.
[9] European Data Protection Supervisor, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit" (https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf), April 11 2017, p.5.

2. **Existence of a legitimate interest:** In order to be able to process data on the basis of Article 6(1)(f) GDPR, it is essential that the purpose pursued for that processing activity is for a legitimate interest, which can pertain to the **controller** or even to a **third party**. As the Article 29 Working Party explains in its guidance, the rule refers, generally, "**to (any kind of) legitimate interest pursued by the controller (in any context)**"[10]. The interest must be **real** and **present**, something that corresponds with current activities or benefits that are expected in the very near future[11]. It must be **sufficiently clearly articulated** to allow a balancing test to be carried out against the interests and fundamental rights of the data subject. And it must be legitimate, in the sense that it must be **lawful, permitted by applicable EU and national law**[12]. The Preamble of the GDPR offers some examples of legitimate interests: preventing fraud[13], direct marketing[14], transmitting personal data within a group of undertakings for internal administrative purposes including the processing of clients' or employees' personal data[15], ensuring network and information security, including preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems[16]. Regardless of these examples, it should once again be emphasized that any kind of legitimate interest pursued by the controller in any context can be taken into account for legitimizing a processing activity under Article 6(1)(f). However, the other two conditions must also be met for the processing to be lawful under this ground: necessity, detailed above, and the balancing exercise, detailed below.

3. **Balancing exercise:** Finally, the mere existence of a real and present, sufficiently articulated legitimate interest is not enough for the processing to be considered lawful under Article 6(1)(f) GDPR. The last element that needs to be complied with is a balancing test between those interests and the interests or fundamental rights and freedoms of the individuals whose data are processed. More weight is added to the latter if the data subject is a child. According to the Article 29 Working Party, the first step in carrying out the balancing test is looking at the nature and source of the legitimate interests on one hand, and the impact on the rights of the data subjects on the other hand[17]. After analyzing the two sides against each other, a provisional balance should be established[18]. The more safeguards the controller can bring towards the protection of the data subject, the more the balance will tip towards the controller[19]. According to guidance from the Preamble of the GDPR, the balancing exercise should also take into account the **reasonable expectations of data subjects**, based **on their relationship with the controller**[20]. For instance, if there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller (an employee), this would help justifying the existence of a legitimate interest[21]. Thus, processing personal data of individuals that have no relationship with the controller will make the balance tilt more towards the interest and rights and individuals. The legitimate expectations of the data subject can be assessed taking into account whether they reasonably expect at the time and

[10] Article 29 Working Party, "Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46", April 9, 2014, p. 13.
[11] Idem, p. 24.
[12] Idem, p. 25.
[13] Recital 47 GDPR.
[14] Recital 47 GDPR.
[15] Recital 48 GDPR.
[16] Recital 49 GDPR.
[17] Article 29 Working Party Opinion on legitimate interests, p. 33.
[18] Idem, p. 34.
[19] Idem, p. 34.
[20] Recital 47 GDPR.
[21] Recital 47 GDPR.

in the context of the collection of the personal data that processing for that purpose may take place[22]. If data subjects do not reasonably expect further processing, meaning processing for an additional purpose than the one for which data have been originally collected, the interests and fundamental rights of the data subject could in particular override the interest of the controller[23]. After all additional safeguards are proposed, the reasonable expectations of data subjects are taken into account, together with the relationship between the data subjects and the controller, and the balance tips in favor of the controller, only then the processing will be legitimized under Article 6(1)(f).

2.3 Consequences of processing personal data on the basis of legitimate interests

Processing personal data on the basis of the legitimate interests of the controller or a third party means that the controller does not have to put in place any other measures to ensure that the processing of those data is lawful. In short, it will not have to worry about compliance with Article 6 GDPR. But it will still have to worry about the rest of the Regulation, starting with the principles in Article 5 – transparency, data minimization, purpose limitation etc., and continuing with the rights of the data subjects, the accountability provisions (on data protection officers, registers of processing activities, data protection impact assessments), security requirements and so on.

Quite importantly, transparency obligations equally apply to processing of data on the basis of legitimate interests as it applies to processing of data on the basis of consent. This means that the data protection notices required under Articles 13 and 14 will still have to be provided and be as detailed as required by those provisions.

Equally, the rights of the data subject are entirely applicable to data processed on the basis of legitimate interests, with one exception (the right to data portability). As such, the rights of access – under Article 15, rectification – under Article 16, erasure – under Article 17, restriction – under Article 18, the right to object – under Article 21 and the right not to be subject to a decision solely based on automated processing, are all applicable to processing of personal data on the basis of legitimate interests.

Of particular significance is the general **right to object**, which only applies to processing of data based on necessity to carry out a task of a public body and necessity for a legitimate interest. Only if the processing activity is based on one of these two grounds, the data subject has the right to object to the processing on grounds relating to his or her particular situation. Once the data subject exercises this right, the controller must interrupt or avoid starting the processing, unless it can demonstrate "compelling legitimate grounds"[24] that override the interests or rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims[25]. As the Article 29 Working Party explained, the controller having to demonstrate compelling legitimate grounds to be able to continue the processing after objection from the data subject should not be seen as contradicting the balancing test, as "it rather complements the balance, in the sense that, where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an additional possibility to object on grounds relating to his/her particular situation"[26].

[22] Recital 47 GDPR.
[23] Recital 47 GDPR.
[24] Article 21(1) GDPR.
[25] Article 29 Working Party, WP251 "Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 2016/679", October 3, 2017, p. 25.
[26] Article 29 Working Party, Opinion on legitimate interests, p. 45.

The **right to data portability** – under Article 20, is the only right of the data subject that does not apply to processing based on Article 6(1)(f). According to the first paragraph of Article 20, the right to data portability only applies where the processing is based on consent[27] or on contract[28]. However, even if the controller is not under an obligation to provide for data portability, the Article 29 Working Party advised that data portability deserves special attention among the additional safeguards which might help tip the balance to be able to use Article 6(1)(f) as legitimate ground for processing[29].

One last consequence should be mentioned – relying on Article 6(1)(f) as legitimate grounds for processing without respecting all the conditions attached to this provision will result in processing personal data without a valid lawful ground for processing, which triggers the maximum tier of fines provided for by the GDPR (20 million EUR or 4% of the global annual turnover)[30]. If the data is processed without a valid legitimate ground, the controller will also be under an obligation to erase the data[31].

2.4 Guidance for specific use-cases issued by Data Protection Authorities for using "legitimate interests"

The Article 29 Working Party and the national DPAs have adopted guidance on specific processing activities and the potential use of the "legitimate interests" ground for their legitimization.

PROFILING	WP29 acknowledged[32] that profiling (that is not based on processing solely done by automated means resulting in legal or significant effects) is capable of being legitimized by Article 6(1)(f) GDPR but warns that this ground does not automatically apply just because the controller or the third party has a legitimate interest. The controller must carry out a balancing exercise to assess whether its interests are overridden by the data subject's interests or fundamental rights and freedoms. The WP29 advises that the following are particularly relevant: • the level of detail of the profile (broad, or segmented, granular); • the comprehensiveness of the profile (does it describe one aspect of the data subject, or a more comprehensive picture); • the impact of the profiling (effects on the data subject); • the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process. • the WP29 suggested that "it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive processing and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering"[33].

[27] Either on Article 6(1)(a) or Article 9(2)(a).
[28] Article 6(1)(b).
[29] Article 29 Working Party, Opinion on legitimate interests, p. 47.
[30] Article 83(5)(a).
[31] Article 17(1)(d).
[32] Article 29 Working Party, WP251rev.01 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 6 February 2018, p. 14.
[33] Idem.

EMPLOYEE DATA (WP29)	WP29 highlighted that in the employment context consent can rarely be deemed "freely given", therefore the processing that is not justified by a legal obligation is more likely to be lawfully grounded on "legitimate interests"[34]. The WP29 highlights several conditions to be met in order for the personal data to be lawfully processed on this ground, related to the "balancing exercise". It is essential that specific mitigation measures are present to ensure a proper balance between the legitimate interests of the employer and the fundamental rights of the employees, especially in the case of monitoring of employees. Such limitations could be: • **geographical:** (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places, sanitary zones and break rooms should be prohibited); • **data-oriented**: (e.g. personal electronic files and communications should not be monitored); • **time-related:** (e.g. sampling instead of continuous monitoring).
EMPLOYEE DATA (Hungary DPA):	The Hungarian DPA released guidance[35] in 2016 about the basic requirements for data processing in the employment context. The guidance covers job applications, fitness checks, whistleblowing, employee monitoring, use of biometric entry systems and investigations. The guidance confirms that employers may not rely on consent as a legal basis for processing employee data due to the subordinate relationship among the employer and employee and must therefore rely on other legal bases such as the legitimate interest test. If relying on this test, the DPA states that the employer must define the legitimate interests pursued, conduct the test, document it and then disclose the result of the test to the employees. Employers must then develop their own internal by-laws respecting data processing activities based on legitimate interests and demonstrate compliance with the law.
FINANCIAL SERVICES	The Spanish DPA issued guidance to the banking industry on legitimate interest and data portability under the GDPR and determined that financial entities can process personal data based on "legitimate interests" for several specific purposes and as long as they comply with transparency obligations and provide for an effective right to object[36]: • **analysis of creditworthiness** (where a product requires risk determination). However, information cannot be collected and used to offer individuals unsolicited products or services; • **transfers of data between companies for prevention of** fraud and within corporate groups for internal administrative purposes, such as processing of customer and employee personal data; • **ensuring network and information security**, such as preventing unauthorized access to communications networks, malicious code, denial of service attacks and damage to computer and electronic communications systems.

3. "Legitimate Interests" in practice

3.1 "Legitimate Interests" in CJEU case-law

The Court of Justice of the EU (CJEU) did not have the opportunity to interpret and apply Article 7(f) of Directive 95/46 many times (which is the corresponding provision to Article 6(1)(f) GDPR). However, there are some cases that provide insight into how the highest Court in the European Union sees the balancing of interests, rights and freedoms of the individual and the legitimate interests of the controller, processor or a third party, as well as how it sees the criteria to lawfully use "legitimate interests" as a ground for processing.

a) *Rigas*[37] – the criteria to lawfully use "legitimate interests" as ground for processing

Facts of the Case:

Case C-13/16 Rigas dealt with the request of a company managing trams in Riga to access from the police the identification and contact details of a person that was involved in an accident that resulted in a damaged tram (a passenger of a taxi that opened the door and scratched the tram). The national police provided access to the name of the passenger, but not his identification number and address, invoking restrictions to disclose information according to the law governing the handling of administrative cases. The tram company challenged the decision of the police and won in first instance. The appeal court asked the Data Protection Authority of Latvia for an Opinion in the matter. The DPA argued that the law governing the handling of administrative cases is special law and it precludes the data protection law. Therefore, the police should apply the restrictions from the special law. Moreover, even if the data protection law would apply, the rules regarding lawful grounds for processing are meant as a "permission" to process personal data, not as an "obligation" to process personal data – so even if the tram company would have a legitimate interest as a third party in obtaining the data from the police, the police is not under an obligation to disclose this data. The appeal court decided to stay proceedings and send a question for a preliminary ruling to the Court of Justice of the EU to clarify what "necessary for the legitimate interests of a third party" means as a lawful ground for processing provided in Article 7(f) of Directive 95/46.

[34] Article 29 Working Party, WP249 Opinion 2/2017 on data processing at work, adopted on 8 June 2017.
[35] November 15, 2016. Hungarian DPA – Basic Requirements for Data Processing in the Employment Context. Retrieved from http://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdfhttp://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf. Available in Hungarian. Related article found at https://www.lexology.com/library/detail.aspx?g=cd530abe-5c1c-4898-9373-5356d03bbb6f.
[36] AEPD, Gabinete Jurídico, Informe 0195/2017.
[37] CJEU, Case C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiks, 4 May 2017.

Main Findings

General principles laid out by the Court (conditions to use Article 7(f))	Application to the facts of the case
The Court clarified that in order for a controller to rely on Article 7(f) as a lawful ground for processing, three conditions must be met[38]: "The **pursuit of a legitimate interest** by the data controller or by the third party" or parties to whom the data are disclosed	The Court found that "there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property **in order to sue that person for damages can be qualified as a legitimate interest**"[39].
"The **need to process personal data** for the purposes of the legitimate interests pursued"	The Court first recalled that "derogations and limitations in relation to the protection of personal data must apply only in so far as is **strictly necessary**". The Court further found that communication of merely the first name and surname of the person who caused the damage does not make it possible to identify that person with sufficient precision in order to be able to bring an action against him. Therefore, "it is necessary to obtain also the address and/or the identification number of that person"[40].
"The **fundamental rights and freedoms of the data subject** do not take precedence"	Regarding the balance of opposing rights and interest at issue, the Court didn't make an exact finding, leaving it to the national court to decide. However, the Court did highlight that this balancing "**depends in principle on the specific circumstances of the particular case**"[41] and that "it is possible to take into consideration the fact that **the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on the possibility of accessing the data at issue in public sources**"[42]. Therefore, whether the personal data is available in public sources or not can be taken into account for the balancing exercise.

[38] Case C-13/16 Rigas, para. 28.
[39] Case C-13/16 Rigas, para. 29.
[40] Case C-13/16 Rigas, para. 30.
[41] Case C-13/16 Rigas, para. 31.
[42] Case C-13/16 Rigas, para. 32.

Conclusion:

- The Court stopped short of deciding whether disclosing of personal data in this case could lawfully rely on necessity for the legitimate interests of a third party, carrying the analysis up until the last point and then leaving it to the national court to decide on the balancing exercise. However, the Court did find, in general, that "Article 7(f) of Directive 95/46 must be interpreted as **not imposing the obligation to disclose personal data** to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive **does not preclude such disclosure** on the basis of national law"[43] (supporting thus the interpretation made by the DPA).

- The Court spelled out the three-tiered test that allows a processing operation, such as disclosure of personal data, to be grounded on the necessity for a legitimate interest – existence of a legitimate interest, necessity of the processing of that data for the purpose of the legitimate interest pursued (under the "strict necessity" test) and the balancing of the rights and interests at stake. It recognized the **establishment of legal claims** as a legitimate interest that can be used under Article 7(f). The Court also provided a criterion to take into account for the balancing test: **whether the data at issue are available or not from public sources.**

b) *Manni*[44] - processing on the basis of legitimate interests may be used to legitimize a processing operation in addition to other grounds

Facts of the Case:

An Italian citizen requested his regional Chamber of Commerce to erase his personal data from the Public Registry of Companies, after he found out that he was losing clients who performed background checks on him through a private company that specialized in finding information in the Public Registry. This happened because the applicant had been an administrator of a company that was declared bankrupt more than 10 years before the facts in the main proceedings. The former company itself was radiated from the Public Registry. The Chamber of Commerce rejected his request and the applicant challenged this decision in Court. The national Court asked the CJEU to clarify whether after a certain period of time has elapsed after a company ceased to trade, and on the request of the data subject, either erase or anonymize that personal data, or limit their disclosure. The Court found in this case that the processing of personal data by the Chamber of Commerce was legitimized by three legal grounds, including necessity for the legitimate interests of third parties.

[43] Case C-13/16 *Rigas*, para. 34.
[44] Case C-398/15 Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni, judgment from 9 March 2017.

Main Findings

General principles laid out by the Court	Application to the facts of the case
The Court reiterated that "all processing of personal data must comply, first, with the principles relating to **data quality set out in Article 6** of the directive and, secondly, with **one of the criteria for making data processing legitimate listed in Article 7** of the directive"[45]	The Court found that three grounds for processing legitimize the processing of personal data by the Chamber of Commerce for the purposes of keeping the Register of companies: • compliance with a legal obligation; • exercise of official authority and performance of a task in the public interest; and • "the realization of a **legitimate interest** pursued by the controller or by the third parties to whom the data are disclosed"[46].
The Court recalled that if the processing is legitimized by the exercise of official authority/performance of a task in the public interest or by the legitimate interest pursued by the controller/a third party, **the data subject has the right to object at any time on compelling legitimate grounds related to his particular situation** to the processing of data (based on Article 14 of the Directive)[47].	The Court first analyzed the purpose of the disclosures made through the Register (and regulated by Directive 68/151) and acknowledged it is **to protect in particular the interests of third parties** in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets. Hence, the basic documents of the company should be disclosed in order for third parties to be able to ascertain information concerning the company, especially particulars of the persons who are authorized to bind the company[48]. The Court considered the wide range of possible scenarios and the considerable heterogeneity in the limitation periods provided for by the various national laws and decided it was "impossible … to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary"[49].
The balancing to be carried out for determining the existence of the right to object "enables **account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation**. Where there is a justified objection, the processing instigated by the controller may no longer involve those data"[54].	

[45] Case C-398/15 Manni, para. 41.
[46] Case C-398/15 Manni, para. 41.
[47] Case C-398/15 Manni, para. 47.
[48] Case C-398/15 Manni, para. 49.
[49] Case C-398/15 Manni, para. 55.
[54] Case C-398/15 Manni, para. 49.

	The Court pointed out that the publication in the Register require "disclosure only for a limited number of personal data items, namely the identity and the respective functions"[50] that the persons held. For the purposes of the right to object, the Court pointed out that in the weighting to be carried out under that provision, in principle, the need to protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market **take precedence**.[51] The Court did not exclude, however, the possibility that there may be specific situations in which "**the overriding and legitimate interests**" of the person concerned justify that access to personal data is limited after the dissolution of a company[52], but emphasized that there may be national legislation limiting or excluding this possibility[53].

Conclusion:

- First, the Court concluded that the persons in the situation of the applicant do not have the right, as a matter of principle, after a certain period of time from the dissolution of the company concerned, to obtain the erasure of personal data concerning them or the blocking of that data from the public. Second, for the purposes of the right to object to this type of processing, it established that the interests of third parties and fair trading take precedence over the rights of individuals "who choose to participate in trade" through a joint-stock or a limited liability company. Last, it also emphasized that there may be individual cases of such persons that justify limiting the access of the public to their personal data.
- This assessment of the Court highlights how important are all the details of a certain processing activity when dealing with balancing of interests and rights. All circumstances matter, from the purpose of the processing, to the category of data subjects, the type of data processed and the interests involved.
- Another take away from this judgment is that the Court acknowledged the possibility that a processing operation can be legitimized by three legal grounds at the same time, including "legitimate interests". However, even if this was not spelled out, it seemed that one of them was considering to be the primary one – necessity for the performance of a task in the public interest.

[50] Case C-398/15 Manni, para. 58.
[51] Case C-398/15 Manni, para. 60.
[52] Case C-398/15 Manni, para. 60.
[53] Case C-398/15 Manni, para. 61.

c) *Ryneš*[55] – home video surveillance could fall under "legitimate interests"

Facts of the case:

Mr. Ryneš installed a video surveillance system outside his home, monitoring the entrance to his home, the public path and the entrance to the house opposite his home. The reason to use the surveillance system was to protect the property, health and life of his family and himself. The camera recorded footage during an incident that involved two suspects breaking the window of his house with an object that was thrown. The footage was used in criminal proceedings as evidence. One of the suspects challenged in Court the legality of the footage, claiming that it constituted unlawful processing of personal data since he didn't consent to it and since he wasn't informed about the existence of the camera. The national Court asked for clarifications from the CJEU before deciding in the matter, asking in particular whether a home video surveillance system falls under the "purely household or personal activity" exemption from the national data protection law.

Main Findings:

General principles laid out by the Court	Application to the facts of the case
1. The provisions of Directive 95/46 "must necessarily be interpreted in the light of the fundamental rights set out in the Charter", therefore the exception provided for in the law for purely domestic purposes "must be narrowly construed"56.	• The Court held that for a processing activity to fall under the household exception, it must be "carried out in the purely personal or household setting of the person processing the data"[57]. • The Court followed that to the extent that video surveillance "covers even partially a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, **it cannot be regarded as an activity which is purely personal or household activity**"[58].
2. The household exception must be narrowly construed also in the light of its own wording – "purely" household or domestic activity, meaning "not simply a personal or household activity"59.	
3. Directive 95/46 makes it possible, where appropriate, to take into account in this case Articles 7(f) – processing on the basis of legitimate interests; 11(2) – where the data is not	• The Court highlighted that the interests pursued by the controller – the protection of the property, health and life of his family and himself – can be taken into account as legitimate

[55] CJEU Case C-212/13 Frantisek Ryneš v. Urad pro ochranu osobnich udaju, 11 December 2014.
[56] Case C-212/13 Ryneš, para. 29.
[57] Case C-212/13 Ryneš, para. 31.
[58] Case C-212/13 Ryneš, para. 33.
[59] Case C-212/13 Ryneš, para. 30.

General principles laid out by the Court	Application to the facts of the case
obtained from the data subject, notice is exempted if it proves to be impossible or it involves a disproportionate effort; 13(1)(d) and (g) – the rights of the data subject may be restricted for prevention, detection and prosecution of criminal offences or the protection of the rights of others.	interests for the purposes of Articles 7(f), 11(2) and 13(1)(d) of the Directive60.

Conclusion:

The Court decided that a home video surveillance system does not fall under the household exemption as long as the camera also covers a public area. However, the Court pointed out that in this particular case the processing activity could be conducted on the lawful ground of necessity for the legitimate interest of the homeowner to protect his property, health and life of his family and himself. Additionally, the Court alluded to the fact that in this particular case several exemptions to the rights of the data subject are applicable, meaning in practice that the data controller wouldn't have to provide notice or grant other specific rights to the data subject.

d) *Google Spain*[61] : the fundamental rights of the data subject generally overrule the economic interest of the controller and the interest of third parties to have access to information

Facts of the Case:

A Spanish citizen asked a newspaper to remove an old article about his personal bankruptcy from its online webpage. He also asked Google to remove the link to that article from the Search Results page that appeared after googling his name. Both organizations rejected the request, which lead the applicant to submit a complaint to the Spanish Data Protection Authority. The DPA decided that the newspaper is not under an obligation to remove the article (on ground of journalistic exceptions), but that Google is under an obligation to remove the link to the article. Google challenged the decision of the DPA in Court, arguing among other things that the Spanish law doesn't apply to it, since it is a company based in California. The national Court decided to hold proceedings and ask the CJEU for clarifications on the interpretation of Directive 95/46 with regard to its jurisdiction and the right to erasure. In delivering the judgment, the CJEU relied primarily on carrying out a balancing exercise between the rights of the data subject and the legitimate interests of Google as the controller, and of internet users as third parties, to rule the processing unlawful and allow, thus, for the right to erasure to take effect. The summary below will focus on these aspects of the case.

[60] Case C-212/13 Ryneš, para. 34.
[61] Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzalez, judgement of 13 May 2014.

Main Findings:

General principles laid out by the Court	Application to the facts of the case
Article 12(b) of the directive guarantees data subjects the right to obtain erasure of data the processing of which does not comply with the provisions of the directive, "in particular" because of the incomplete or inaccurate nature of data. This means that the "non-compliant nature of the processing … may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data"[62], including non-compliance with Article 6 (data quality principles) and Article 7 (lawful grounds for processing).	The legitimation of processing such as that at issue in the main proceedings carried out by an internet search engine operator "is capable of being covered by the ground in Article 7(f)"[63] – necessity for the legitimate interests of the controller or a third party.
The Court established that "all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the directive"[64].	
Application of Article 7(f) "necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter"[65].	Processing of personal data such as that at issue in this case "carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the

[62] Case C-131/12 Google Spain, para. 70.
[63] Case C-131/12 Google Spain, para. 73.
[64] Case C-131/12 Google Spain, para. 71.
[65] Case C-131/12 Google Spain, para. 74.

	interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines66". With regard to the legitimate interests of the controller to process that data to carry out its business, the Court found that, given this potential serious interference, "it is clear that it (the interference – n.) cannot be justified by merely the economic interest which the operator of such an engine has in that processing"67. With regard to the legitimate interests of third parties ("internet users") to have access to that information, the Court found that the rights of the data subject protected by Article 7 and 8 of the Charter "override as a general rule, that interest of internet users"68. However, the Court highlighted that this balance may depend in specific cases "on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life"69. The Court also found that the ground in Article 7 justifying the publication of a piece of personal data on a website does not necessarily coincide with that which is applicable to the activity of search engines70. Even when they do coincide, "the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and [Article 14(1)a] of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same"71.

[66] Case C-131/12 Google Spain, para. 80.
[67] Case C-131/12 Google Spain, para. 81.
[68] Case C-131/12 Google Spain, para. 81.
[69] Case C-131/12 Google Spain, para. 81.
[70] Case C-131/12 Google Spain, para. 86.
[71] Case C-131/12 Google Spain, para. 86.

Conclusion:

The assessment of the balance between the legitimate interests of the internet search engine providers and of internet users, on one side, and the rights of the data subject, on the other side, in the context of complying with Article 7(f) of Directive 95/46, had a significant role in the outcome of the *Google Spain* case. Thus, in order to ascertain the existence of the right to erasure (the right to be forgotten) in this particular case, the Court analyzed whether the processing of personal data at issue was lawful. It considered that the lawful ground for processing in this case was most likely the "legitimate interests" ground. Carrying out the balancing exercise, it found that the rights of the data subject outweigh the legitimate interests of the controller and the third parties in this case, which meant that the processing was not compliant with the requirements of Article 7(f). Since the processing was not lawful, this allowed for the right to erasure to be affirmed in this case.

e) *ASNEF*[72] - the use of "legitimate interests" ground must not be limited by national law

Facts of the Case:

In ASNEF the CJEU was asked to interpret Article 7(f) of Directive 95/46 in the context of the Spanish transposition law, which added a condition to this lawful ground that restricted the possible use of "legitimate interests" only for those personal data that were available in public sources. The challenge was brought to Court under administrative proceedings by two professional associations (one of them concerned with financial and credit institutions and the other one with e-commerce and direct marketing), who also wanted to ascertain whether Article 7(f) of the Directive enjoys "direct effect" (meaning that the provision of the Directive could be directly applicable, instead of the national law transposing it).

Main Findings:

General principles laid out by the Court	Application to the facts of the case
The harmonization of national laws transposing Directive 95/46 is not limited to minimal harmonization, but "amounts to harmonization which is generally complete"[73]. Additionally, the objective of the directive is ensuring an equivalent level of protection in all Member States, which means that Article 7 sets out "an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful[74].	The Court held that Member States cannot add new principles relating to the lawfulness of the processing of personal data to Article 7 of Directive 95/46 or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7[75].

[72] CJEU, Joined Cases C-468/10 and C-469/10 ASNEF and FECEMD v. Administraction de Estado, judgment of 24 November 2011.
[73] Joined Cases C-468/10 and C-469/10 ASNEF, para. 29.
[74] Joined Cases C-468/10 and C-469/10 ASNEF, para. 32.
[75] Joined Cases C-468/10 and C-469/10 ASNEF, para. 30.

Article 7(f) "sets out two cumulative conditions that must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of personal data must be necessary for the purposes of the legitimate interests pursued by the controller or third party; and, secondly, such interests must not be overridden by the fundamental rights and freedoms of the data subject"[76].	The Court held that Article 7(f) precludes any national rules which, in the absence of the data subject's consent, impose requirements that are additional to the two cumulative conditions it requires[77], such as requiring that the personal data must be available in public sources in order for a controller to be able to rely on the "legitimate interests" ground.
In relation to the balancing which is necessary pursuant to Article 7(f) of Directive 95/46 it is possible to take into consideration the fact that **the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources**[78].	Unlike the processing of data appearing in public sources, the processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter must be properly taken into account by being balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed[79]. The Court held that "there is nothing to preclude Member States … from establishing guidelines in respect of that balancing"[80].

Conclusion:

The Court concluded that Member States cannot adopt national rules transposing Article 7(f) of Directive 95/46 by adding the condition that personal data must be available in public sources in order for the "legitimate interests" ground to be lawfully used. However, the Court did note that Member States can adopt guidelines for the balancing exercise to be conducted between the interests of the controller or third parties and the rights and freedoms of the data subject, favoring the use of personal data available in public sources for this lawful ground to be used.

[76] Joined Cases C-468/10 and C-469/10 ASNEF, para. 38.
[77] Joined Cases C-468/10 and C-469/10 ASNEF, para. 39.
[78] Joined Cases C-468/10 and C-469/10 ASNEF, para. 44.
[79] Joined Cases C-468/10 and C-469/10 ASNEF, para. 46.
[80] Joined Cases C-468/10 and C-469/10 ASNEF, para. 46.

3.2 Cases of unlawful use of "legitimate interests" as ground for processing, at Member State level (EEA)

Processing activity & Source	Summary
Publication of WHOIS-data of domain name registrants by Dutch registries for transparency purposes **Source:** Data Protection Authority, The Netherlands (October 30, 2017)[81]; Article 29 Working Party (Letter from 2003, Letter from December 2017)[82]	A Dutch registry asked the Dutch DPA if it is legal to publish all WHOIS data on the internet, giving unlimited access to all data. The Dutch DPA, relying also on recommendations of the Article 29 Working Party, replied that such a publication is in breach of data protection law, as none of the lawful grounds for processing is applicable, including necessity for a legitimate interest. The DPA considers that consent cannot be used because it wouldn't be freely given; necessity to enter a contract cannot be used either, as the individual domain name holders are not a party to the contract between ICANN and Registries. Legitimate interest cannot be used because the publication concerns all personal data and unlimited access to such data. **Comment:** The Dutch DPA refers to layered access as an alternative that would allow processing of WHOIS data to be lawful. Even if this is not stated in the press release, it seems that if the registries would publish partial data and would provide layered access to the data, the legitimate interest ground could be legally used.
Using key-logger software in employment context for monitoring purposes **Source:** Federal Labour Court, Germany (July 27, 2017)[83]	A company installed software on an employee's computer that recorded all the keyboard inputs and produced screen shots on a regular basis. He then filed suit against the Company after the termination of his employment. The lower courts granted the wrongful termination lawsuit against the Company and the Company appealed the decision. In the Appeal judgment, the Court found that this monitoring technique is too intrusive to be justified by the legitimate interest of the Company. According to the Court, "data collection by a key-logger interferes massively with the right of the person concerned to informational self-determination. It captures and stores - all inputs are irreversible to the user - via the keyboard of a computer, including the time of entry and the time interval between two inputs. The data obtained in this way make it possible to create a nearly comprehensive and complete profile of both the private and official use of the data subject. Not only stored final versions and possibly intermediate drafts of certain documents are visible, but it is possible to follow every step of the user's working method. In addition, special categories of personal data or - so in case of dispute - other highly sensitive data such as user names,

[81] Autoriteit Persoonsgegevens (2017, October 30). Dutch DPA: unlimited publication of WHIS – data violates privacy law. Retrieved from https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-unlimited-publication-whois-data-violates-privacy-law

[82] Article 29 Working Party (2003, June 13). Opinion 2/2003 on the application of the data protection principles to the Whois directories. Retrieved from http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp76_en.pdf

[83] 2016 (June 6). Haftung des Arbeitgebers für Impfschäden. Retrieved from http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&Datum=2017&anz=31&pos=0.

Processing activity & Source	Summary
	passwords for protected areas, credit card information, PIN numbers, etc. are logged, without this being necessary for the purposes of monitoring and surveillance. Likewise, the affected employee has neither cause nor the ability to identify certain content as private or even personal and thus possibly withdraw the access of the employer. This already far overcoming interference in the right to informational self-determination of the person concerned is further intensified if - as here - regular screenshots are made". **Comment:** The Court highlights several aspects of the processing activity that are too intrusive – making regular screenshots, the fact that the employee does not have the possibility to identify certain content as private, the fact that the keylogger also captured special categories of data that were not necessary for the monitoring purposes for which the system was put in place. This could mean that measures that would mitigate these aspects could be used to rebalance the relationship between the interests of the controller and the rights of the person.
GPS tracking of a vehicle as part of a private investigation for private reasons, including economic interests and matrimonial disputes **Source:** Federal Court of Justice, Germany (June 4, 2013)[84]	The Federal Court of Justice upheld the decision of a lower court which sentenced the owner of a detective agency and one of its employees because they had installed concealed vehicle-mounted GDS receivers for various clients in order to monitor the movements of targeted individuals. The motives of the clients were primarily about economic and private interests, some of which concerned matrimonial disputes. The Court referred in its judgment to the balancing exercise of the conflicting interests in the case and held that the defendants could have processed the GPS information only with a strong legitimate interest in the data collection, such as self-defense. However, tracking individuals by GPS for private interests falls short of the required threshold in the law. **Comment:** In this case, the Court considered that the legitimate interest invoked was not strong enough, giving "self-defense" as an alternate acceptable legitimate interest. Therefore, mitigation actions do not seem to potentially have significance.
Cross-checking between CCTV images capturing license plates and a "blacklist" database containing	A security company and a gas companies' association submitted an application to the Swedish Data Protection Authority for an exemption from the Data Protection Act to process personal data for the purpose of combatting an industry-wide problem of fueling and then fleeing the gas station without paying. Gas stations justified their legitimate interest stating that they experience more than 100,000 incidents of gas theft per year, resulting in a total annual loss of SEK 44 million (approximately USD 5.4

[84] Decision on Surveillance of Persons by Means of Vehicle-Mounted GPS Devices - Supreme Court of Germany Press Office. Retrieved from http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2013&Sort=3&nr=64248&pos=2&anz=97.

Processing activity & Source	Summary
criminal record and previous fleeing without paying incidents in gas stations for preventing "fleeing without paying incidents" **Source**: Data Protection Authority, Supreme Administrative Court of Sweden (April 28, 2016)[85]	million) for gas station owners at all 1,400 stations. The system would involve a dedicated camera at the gas station entrance that automatically reads the vehicle license plate number, a comparison of the number with others registered in the security company's database (containing a list of vehicles and related data). If there is a match, the gas station employees would require prepayment from the customer and a subsequent notice is sent to the vehicle owner that an incident occurred. Unmatched data would be immediately deleted. This proposal was first rejected by the DPA, the main reason being that the system also involved processing of criminal offense data. The DPA noted that the industry had a legitimate interest in combatting the problem of payment evasion, however, the use of "blacklists" presents risks in the form of incorrect registry entries (inaccuracy) and large-scale processing (a database containing large volume of personal data). Another reason for the denial was that **the proposal did not justify the comprehensive recording and processing of personal data for such a blacklist**, as the problem could be solved through the imposition of mandatory prepayment. The decision of the DPA was challenged in Court. The first instance Court upheld the decision, the Appeal Court canceled the Decision (arguing that the interference with the right to privacy was proportionate and struck a balance between the interests of the gas stations and the protection against a violation of privacy). This decision was brought by the DPA in front of the Supreme Administrative Court (a Court of last resort). The Supreme Administrative Court upheld the initial decision of the DPA, ruling that the proposal does not justify the infringement of privacy caused by the processing in light of Section 21 of the Data Protection Law, which prohibits the processing of criminal offence data. Such processing is limited to law enforcement authorities and regulated in special legislation. Other **aspects that do not justify the interference are the risk of inaccuracy, the comprehensive system and number of companies involved and significant related privacy risks.** **Comment:** A legitimate interest was also identified in this case and acknowledged by the DPA in its initial decision and then by the Supreme Court which upheld that decision. The main condition that seems to not have been fulfilled here is the "necessity" condition, since the DPA argued that the comprehensive recording and processing are not justified by the purpose of the processing activity. Overall, the intrusiveness of the measures proposed was not proportional to the purpose, even if the controller had a legitimate interest at stake.

[85] Swedish Data Inspection Board v. Amos Forest Service AB - Appeal No. 13555-13 - Administrative Court of Appeal in Göteborg. Retrieved from http://www.datainspektionen.se/Documents/beslut/2015-06-10-kammarratten.pdf.

Processing activity & Source	Summary
Combining of personal data obtained through several different services and products provided by the same company, for four purposes: personalization of requested services, product development, display of personalized ads and website analytics **Source:** Data Protection Authority, The Netherlands (Investigation into the combining of personal data by Google, Report of Definitive Findings. November 2013)[86]	The Dutch DPA investigated a Company for combining personal data obtained through the use of several of the Company's services and products (internet search engine, video streaming webpage, web browser, online maps, e-mail). The investigation looked at four purposes for which the data were combined and that were disclosed in the privacy policy of the Company: personalization of requested services, product development, display of personalized ads and website analytics. The DPA concluded that the processing was not based on valid consent, since consent was not unambiguous and was not sufficiently informed. Subsequently, the DPA analyzed to what extent the company lawfully processed data on the ground that this was necessary for its legitimate purposes. The DPA acknowledged that data controllers can have legitimate interests in developing new services on the Internet for which there is demand. However, they must take into account the impact these services will have on the individual privacy of the data subjects. In order to be able to rely on the "legitimate interests" ground, the data controller must build in safeguards to prevent any disproportionate disadvantage. Careful data processing requires that data subjects be actively informed about the recording of personal data relating to them and the specific purposes for which these data are collected and processed. The DPA found that the Company's legitimate interest does not outweigh the data subject's right to protection of their personal data and privacy, due to the nature of the data (i.e. some of these data are of a sensitive nature, such as: payment information, location data, and information on surfing behavior across multiple websites), the diversity of the services that serve entirely different purposes from the point of view of users (e.g. browsing, email, viewing videos, consulting maps), the lack of adequate and specific information, and the lack of effective opt-outs. When assessing the impact of the data processing activities on the data subject's right to respect for private life, the DPA also took into account the considerable share of the market that the various services of the company had in the Netherlands. The DPA found that it was almost impossible for a Dutch internet user not to interact with the Company's services, even without opening a user account, be it via the search engine, using the online maps, streaming videos or even passively through third-party websites and analytics cookies. The DPA found that **the Company has failed to put adequate safeguards in place to ensure that the combining of data is strictly limited to what is necessary in the context of the legitimate purposes pursued.**

[86] Dutch Data Protection Authority. (2013 November). Investigation into the combining of personal data by Google, Report of Definitive Findings. Informal Translation. Retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_rap_2013-google-privacypolicy.pdf.

Processing activity & Source	Summary
	Comment: In this case, the DPA acknowledged that the controller had a legitimate interest for the processing of personal data. However, the "necessity" requirement was not met and there was a lack of sufficient measures that would safeguard the right of the data subjects.
Retaining banking data by an online retailer in order to facilitate later payments and optimize business transactions **Source:** Data Protection Authority, France Deliberation No. 2012-214 (July 19, 2012)[87]	The French Data Protection Authority investigated an online retailer with regard to its practice of retaining banking data of customers longer than necessary for the transaction to take place. The investigation showed that the company retained banking data by default, at the end of every transaction (name of cardholders, card number, validity date and some CVV codes; the information referred to both valid and expired cards). The retailer argued that it retained the data on two lawful grounds – necessity for entering or for the performance of a contract and necessity for its legitimate interest. Specifically, the legitimate interests invoked were facilitation of later payments and optimization of business transactions. The DPA found that retaining the banking details goes beyond the execution of a service contract for an online sale, since the electronic wallet functionality of the website is for customer convenience in facilitating the conclusion of non-specific hypothetical future sales. The DPA also found that processing was not lawfully based on the "legitimate interests" ground. The DPA acknowledged that there was a legitimate commercial interest of the retailer in facilitating later payments and optimizing business transactions. However, this interest must be balanced against the rights of the persons concerned. The DPA took the view that given the sensitivity of banking data, the right of the data subject to have the data deleted after being retained for a period of time cannot be considered an adequate guarantee for the rights and interests of the data subjects. **The banking data were not subject to any final purge, manual or automated, but it was subject to archiving depending on several criteria, such as the end of the warranty period.** The DPA clarified that the company would be entitled to retain the data maximum 13 months, following national legislation in the financial sector (this corresponds to the period necessary to defend against potential actions taken by banks that have had to repay customers on the basis of Article L-133/24 of the Monetary and Financial Code). The company also failed to take appropriate security measures – the credit card details of millions of customers were stored in clear text, in a single database, giving rise to a risk that the data would become accessible through malicious employees or external intrusions. **Comment**: The controller had a legitimate interest for processing of personal data in this case. However, it did not take enough measures to make sure that the rights of the data subjects are protected, as part of the "balancing

[87] Retrieved from http://www.cnil.fr/la-cnil/actualite/article/article/avertissement-pour-la-societe-fnac-direct-en-raison-de-manquements-dans-la-conservation-des-donne/ Press Release available in French

Retrieved from http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2012-214-FNAC.pdf Deliberation available in French

Processing activity & Source	Summary
	exercise". The DPA gave concrete examples of what those measures should have been and even specific guidance on what retention period for the financial data would have been acceptable.
Processing personal data in order to provide free texting service **Industry**: Website operator **Source:** Data Protection Authority, Hungary, November 2, 2017[88]	The Hungarian DPA investigated the personal data handling practices by a company operating a website which offered free texting services. An individual reported that the company failed to remove his email address from their records. The Company argued that it had removed the email address from its website so that no one else could view it but that it needed to retain the information in order to contact the individual. The DPA stated that an organization cannot process personal data without a valid legal ground. It asserted that where the controller relies on legitimate interest it must first do an assessment of its legitimate interest taking into consideration the fundamental right of the data subject, particularly in the case where a data subject may revoke previous consent. The organization must further notify the data subject so that they can clearly identify which legitimate interest is proportionate to the handling of their personal data without consent. The DPA found that the Company failed to comply with articles 17 and 18 of the Hungarian Data Protection Act ("Act"): It did not notify Complainant of the reasons it refused to comply with the erasure request; and It's reasoning for refusal based on legitimate interest cannot be relied on, since it failed to complete a legitimate interest assessment. The Company was ordered to modify the information provided to data subjects on its website and to delete the personal data of any user for which it did not have consent to process but instead relied on legitimate interest. **Comment:** It appears that the Company could have relied on legitimate interests in this circumstance if they have provided notice of this legal basis for processing personal data and if they had internally conducted a legitimate interest assessment. This highlights the importance of documentation of maintaining internal documentation of the legitimate interest assessment.
Creation of a mega database for purposes of selling to third parties	This Court decision involved the appeal of a fine imposed by the Spanish DPA regarding the processing of personal data without the data subject's consent. In this case, an organisation created an automated data file with the personal data of almost 37 million Spaniards. The data included ID number, current and previous addresses and date of birth. The data had been collected from the electoral and municipal registers (which were not publicly available sources) and a credit reporting entity. The purpose of the database was to commercialize the data by selling it to third parties such as debt collectors,

[88] DPA Hungary - NAIH 2017-1-6-V - Regarding the Data Handling Relating to the Website mobiltelo.hu. Retrieved from http://www.naih.hu/files/Adatved_jelentes_NAIH-2017-1-6-V.pdf. Available in Hungarian

Processing activity & Source	Summary
Source: Spanish National Court of Appeals, June 6, 2012[89]	fraud investigators and others would be able to search the website to find personal data about the data subjects location. The company allegedly engaged in two offenses: 1. The breach of the principle requiring consent for the processing of personal data under Article 6.1 of the Spanish Data Protection Act and transferring data without consent in violation of Article 11.1 of the Act. The Court found that the data was collected without consent. The company invoked Article 7 (f) of the Directive 95/46/EC stating that processing of personal data, including by third parties, is necessary for the purposes of a legitimate interest of the data controller or the third party. The Court held that there was nothing in the case that showed the date collection was justified by a legitimate interest. In its reasoning it noted that the municipal register and electoral roll are not public sources and while the telephone directory is a public source, the directory does not list all of the personal data that was collected (such as ID number or birthday). The creation of a mega file such as the database in question, with the intention of commercializing it and providing the information obtained, violated the privacy rights of those affected. The court did reduce the fines for the violations from approximately €360,000 to €80,000, since a law passed subsequent to the Data Protection Authority's original decision reduced the amounts that could be imposed for serious offenses and reduced the gravity of one of the offenses from "very serious" to "serious". **Comment:** The court provided an example of a purpose that met the legitimate interest criteria: where a particular company needs to find out the address of a creditor in order to arrange the collection of a debt.
Use of CCTV footage in disciplinary hearings Data Protection Commissioner of Ireland, Annual Report 2013, Case Study 9[90]	The DPC received a complaint stating that a supermarket had instructed a third party to remove a CCTV hard-drive. The hard drive contained CCTV footage of the complainant's image from the store where the complainant worked as store manager. The complaint stated that no member of the supermarket staff accompanied this third-party contractor during the removal. The complainant alleged that the supermarket viewed had three weeks of CCTV footage. The footage contained the complainant's image and the supermarket used this CCTV footage to ground a disciplinary hearing against the complainant. The complaint further stated that at no point had the complainant been consulted in relation to the removal, viewing or processing of the footage. The key issue before the DPC was consideration of whether the supermarket had acted in accordance with the requirements of the applicable law when it

[89] Saberlotodo Internet, S.L. - Judgment of June 6, 2012 - Spanish National Court of Appeal. Retrieved from https://www.iberley.es/jurisprudencia/sentencia-administrativo-an-sala-contencioso-sec-1-rec-594-2009-06-06-2012-13777081

[90] Twenty-Fifth Annual Report of the Data Protection Commissioner 2013, p. 61 https://www.dataprotection.ie/docimages/documents/Annual%20Report%202013.pdf

Processing activity & Source	Summary
	processed the CCTV footage which contained images of the complainant, specifically Section 2A(1)(d) of the Acts which provide that a data controller shall not process personal data unless "the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.". The DPC determined that the use of CCTV in employment situations should only be used for stated valid purposes, such as security. It should not be used for employee monitoring, and policies should be in place to ensure proportionality and transparency in the workplace. However, the DPC considered that, when the supermarket viewed the CCTV footage for the period, it did so in the pursuit of its own legitimate interests and in this instance found there was no contravention of the Act.
Processing data for rental applications Data Protection Commissioner of Ireland, Case Studies 2014[91], Case Study 5	The DPC received a complaint from a prospective tenant regarding the collection of bank details, PPS numbers and copies of utility bills by a letting agency when applying to rental property. In reviewing the compliant, the DPC considered that this was a classic example of the temptation of some data controllers to collect a whole range of personal data in case they might need it in the future. The DPC determined that there is no need to ask for bank details, PPS numbers and copies of utility bills at the application stage. However, once an applicant has been accepted for the apartment, the data controller can request copies of bank details, PPS numbers and copies of utility bills to show that a tenant has a bank account that they can pay their rent. Data controllers must be careful not to ask for overly broad and unnecessary data collection practices.
Processing data for addressing data at security problems at apartment complexes Data Protection Commissioner of Ireland, Annual Report 2013, Case Study 4[92]	The DPC received a complaint from a tenant of an apartment complex who indicated that the management company of the complex was in the process of introducing a new key pad access system to resolve serious security issues in the complex. The management company was requesting a copy of passport/driving license, PPS Number, emergency contact details, vehicle details, employment details and a copy of a current lease/tenancy agreement. The management company explained that they sought this level of detail because in the past, information given to it by landlords did not always align with who was living in the complex. The DPC determined that data controllers cannot ask for excessive personal information (i.e., passport/driving license, emergency contact details, vehicle details, etc.) in order for tenants to have access to security system at building. The DPC stated that the Data Protection Acts require an appropriate balance by struck between the legitimate interests of a data controller to protect its business and the privacy considerations of the users. The DPC informed the company

[91] Data Protection Commissioner, Case Studies 2014 https://dataprotection.ie/viewdoc.asp?DocID=1613&ad=1#20145
[92] Ibid. , f

Processing activity & Source	Summary
	that any information collected should be adequate, relevant and not excessive in relation to the purpose for which it was obtained and held and determined that amount of information requested was excessive in relation to the introduction of a new access system. **Note:** in this case, when the management company then reduced the amount of personal information it required from tenant limiting it to emergency contact details, vehicle details and a copy of a current lease/tenancy agreement in order to register for the new access system, and notified tenants as such. The DPC reviewed the new process and considered the information now to be fair and reasonable for the purposes for which it was sought.
Collecting medical information as part of a vaccination program DPA Slovenia - Opinion 0712-1/2015/3046[93]	The DPA received a complaint from a parent that their child had brought home an HPV vaccination form and declaration statement from school which contained questions such as: does your child currently have a disease and if so, which one; and currently take any medication and if so, which one. has your child ever had a severe reaction after vaccination and if so, what was the reaction. The parent asked whether the school had a legitimate interest in the data they were asking for. The DPA determined that there does not appear to be a legitimate basis on which to process the health data under the Data Protection Act; consent was not asked, the processing is not being performed by healthcare workers, and a public interest exemption does not apply (the vaccination is voluntary, not mandatory).
Psychological testing as a tool for employee development and professionalism DPA Netherlands, Final Report[94] of Findings - on Psychological	The Dutch DPA assessed psychological tests and staff assessments being conducted on employees of a youth agency for compliance with data protection laws. It found that an organization's psychological assessments of its employees violated the Data Protection Act since there was no lawful basis for processing based on consent (consent was not freely given since employees that refused testing may be subject to dismissal, and the ability of management to exempt some employees from testing is irrelevant) or the legitimate interests of the organization (the interest in staff professionalism and management could be achieved through other measures, such as

[93] DPA Slovenia - Opinion 0712-1/2015/3046 - Collection of Vaccination Statements from Schools https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1%5BshowUid%5D=2664&cHash=19b6335c9fb90fde67f3aca5ccc2bb33 Available in Slovene

[94] College Bescherming Persoonsgegevens, Netherlands - Final Report of Findings - on Psychological Tests of Employees by the Youth Care Agency of North. Press release retrieved from Brabanthttps://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-gegevens-psychologische-test-werknemers-strijd-met-wet-verzameld.
Final report retrieved from https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2012_jeugdzorgnb.pdf

Processing activity & Source	Summary
Tests of Employees by the Youth Care Agency of North Brabant,	specialized courses and the personal data collected were sensitive, relating to psychological condition).
Processing of telemetry data to fix errors, keep devices up to date and improve products and services DPA Netherlands, Summary of Investigation, August 2017[95]	In this investigation, the Dutch DPA investigated several versions of Windows 10 operating system and found that developer failed to obtain valid consent for the collection and processing of telemetry data because users are not sufficiently informed what is being collected and how it is being used (users are provided with general information), and users must actively opt-out of settings meant to capture sensitive data by default. The developer could not rely on the legal grounds of necessary for "a legitimate interest" or "the performance of an agreement" because: it infringes the Telecommunications Act by not obtaining consent prior to the collection of the data; it processes the data for different purposes and has not demarcated what data it processes for each of those purposes; and the interest of the developer in processing sensitive data does not outweigh the right to protection of the private life of users.
Video surveillance of a dance floor at a night club DPA Norway - Decision 14-01190-8[96]	The DPA of Norway conducted an investigation into the use of video surveillance by a restaurant. The restaurant consisted of four floors and had a total of 19 cameras divided into the following categories: traditional surveillance, where the cameras are easily noticeable masked surveillance that resembled alarm sensors; and covert surveillance that are impossible to spot. It found that article 8 of the Personal Data Protection Act provides that personal data may be processed to enable the controller to protect its premises if there is a legitimate for processing. It determined that that the use of video surveillance outside the restaurant to monitor traffic and security is justified, however, this is a task that needs to be done by the police and not a private establishment. Further, the privacy of customers visiting nightclubs and restaurants outweighs the privacy of customers visiting traditional stores and the restaurant has no justification of having video surveillance on the dance floor.

[95] https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10 Press Release https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf Report

[96] Datalisynet, Norway - Decision 14-01190-8 - Cases of Hidden Video Camera Surveillance. Retrieved from https://www.datatilsynet.no/globalassets/global/regelverk-skjema/avgjorelser-datatilsynet/tilsynsrapporter/2015/15-00209-10-kontrollrapport-ankerskogen.pdf

Processing activity & Source	Summary
Transferring personal data to another entity for marketing purposes DPA Poland, Investigation of 20 banks and 9 credit unions, 2017[97]	The DPA conducted an investigation of 20 banks and 9 credit unions to verify compliance with the Act on Protection of Personal Data. It examined a verification of the companies' compliance of personal data processing related to the conduct of targeted marketing to consumers. It looked at the legal framework: Article 7(5) of the Act on Protection of Personal Data states that the data subject consent can be revoked at any time; and Article 23(1) states that personal data processing is permitted if necessary for the legitimate interests of the controller provided the processing does not violate the rights and freedoms of the data subjects. It stated while personal data may be processed for marketing purposes without consent if there is a legitimate interest there is no legal basis that permits transferring personal data to another entity for marketing purposes without consent of the data subject.
Call recordings for purposes of employee training and quality control DPA Sweden, Decisions 120-2016 and 121-2016 [98]	The Swedish DPA investigated how two telecom companies handled recordings of customer calls to their call centers. It examined the practice of recording calls at random for the purposes of employee training and quality control. It further examined the practice of recording for the purposes of documenting the agreement by the customer for a contract. Both companies were ordered to cease processing customer's data through the random recording of phone calls or better inform the customer of the purposes of processing. One company was further ordered to better notify customers of recording for contractual purposes. **Random recordings for purposes of employee training and quality control:** It was found that the personal data recorded in the calls appeared to be relatively harmless and the data controllers had legitimate interests in personal data processing such as employee training, quality control and improving customer's experience. However, it was difficult to predict which personal data will be processed because the whole call was recorded, therefore, the legitimate purposes did not outweigh customers privacy and therefore there was no legal basis for the recording of customers phone calls. The callers were told that their calls might be recorded, however they were not told the purposes of the recording or provided any other information in order to exercise their rights.

[97] DPA Poland - Banks Mistakenly Formulate Consent Clauses for Personal Data Processing for Marketing Purposes. Retrieved from https://giodo.gov.pl/pl/259/10003. Available in Polish.
[98] https://www.datainspektionen.se/Documents/beslut/2016-05-12-telia.pdf

3.3 Cases of lawful use of "legitimate interests" as ground for processing, at Member State level (EEA)

Processing activity & Source	Summary
Criminal records accessed for background checks for employment purposes by specialized company **Source:** Data Protection Authority, Netherlands (May 20, 2015)[99]	The Dutch DPA authorized the use of criminal records as part of background checks conducted by a Company specializing in background checks provided as a service for employers. The DPA acknowledged that criminal records information belongs to the category of sensitive data and its processing is prohibited as a rule by the national data protection law. One exception allowed in the law for processing criminal records is, nevertheless, "assessing an application by a data subject in order to make a decision about them". The DPA held that the Company specializing in background checks can rely on legitimate interests as a lawful ground for processing only to the extent its clients had a legitimate interest to receive a Background profile of job candidates. Following assessment of internal rules and procedures of the Company, the DPA was satisfied that the Company has set up its working method in such a way that a background check is executed after the Company has satisfied itself that the client has a legitimate interest in the intended background check or is subject to a legal obligation to execute a check. Therefore, the DPA decided that the Company may lawfully process criminal records data acting as a third party for the employer, given that the employer has a legitimate interest ensuring that employees being hired meet its hiring requirement.
Monitoring access of employees to the company's (a bank) information systems to aid in the protection of confidential economic information and to ensure secure and smooth operation of IT systems **Source:** Data Protection	A bank from Monaco asked for an authorization of the Data Protection Authority for an employee-monitoring program used to automatically trace access to its IT system. The DPA considered that the processing operation can lawfully be grounded on the "legitimate interests" basis provided by the national law. The legitimate interest of the company in this case is to monitor and audit employee access to the internal information system and to protect confidentiality of economic information. The DPA considered that the features of the audited program allow the bank to lawfully process employee data on this ground: the data collected is relevant, adequate and not excessive (name, job title, user ID and password, connection identifiers, date and time of access and nature of the action carried out by the employee), employees are informed about this monitoring through the employment contract, the data can only be disclosed to judicial authorities for the purpose of investigating or prosecuting an illegal activity and to Circuit Monitoring and Information Service Financiers, access rights to the logging data are limited and clearly set out and the data retention policy

[99] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ontwerpbesluit_adecco.pdf

Processing activity & Source	Summary
Authority Authorization Decision, Monaco (April 19, 2017)[100]	for employee data is clear and provides for appropriate time limits (data on identity, education and qualifications is retained for 3 months after the employment relationship ended; the employee's electronic identification data is only retained for the duration of the employment relationship and the system traceability data is retained for one year).
Disclosure of health data by a hospital at a request of a defense attorney for litigation purposes **Source**: Data Protection Authority, Greece (Decision 98/2015)[101]	A hospital asked the Greek Data Protection Authority if it is allowed to disclose medical information about a patient to a law firm asking for access. The law firm requested information regarding a patient's stay at the hospital (date and length of time) and medical condition, with the justification that the information is necessary in an open litigation initiated by the patient against the law firm's client. The patient claims damage of 14.500 euro alleging building negligence led to his broken arm and hip. The DPA decided that disclosure of sensitive records is permitted in this case. It argued that under the national data protection law, such disclosure is allowed in exceptional circumstances, one of which is for litigation purposes. The DPA found that the third party to whom the disclosure is made has a legitimate interest in this processing, since the disclosure of data is proportionally necessary for rebuttal of allegations by the data subject against their landlord made in the lawsuit. The DPA also found that such disclosure is lawful only if it is subject to giving notice to the data subject (in this case, the hospital had announced the data subject already about the existence of the request of the law firm).
Disclosure of personal data to a debt collector concerning a debt of the data subject towards the controller **Source:** Data Protection Authority, Bulgaria (July 21, 2014)[102]	An individual complained to the Bulgarian Data Protection Authority that a telephone service provider disclosed personal information in her customer file to a debt collection agency and alleged that such disclosure was made without her consent, in violation of the national data protection law. The DPA opened an investigation and found that there was a contract between the Complainant and the telephone service which had a clause stipulating that personal data could be disclosed to a third party for collection of overdue accounts. According to the assessment of the DPA, the service provider had a legitimate interest in collecting money owed by the Complainant under that contract. Thus, the DPA concluded that the telephone service provider lawfully disclosed the Complainant's personal information to the debt collector, as the disclosure had two lawful grounds for processing – necessity for the performance of a contract and the legitimate interest of the controller.

[100] https://www.ccin.mc/images/documents/18a57b936b7809a531f0dd12c5c57d67-Delib-2017-068-Andbank-habilitations.pdf
[101] http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=4,108,123,217,31,201,206,75
[102] https://www.cpdp.bg/index.php?p=element_view&aid=1486

Processing activity & Source	Summary
Sending electoral e-mails to all members of a professional association by a candidate to the presidency of that association **Source:** Administrative Court, Spain (May 31, 2012)[103]	The Data Protection Authority fined with 2000 euros a candidate to the presidential election of a professional association for sending electoral e-mails to all members of that association without previously obtaining consent to obtain and use their e-mail addresses for electoral purposes. The candidate challenged the decision in administrative Court (Audiencia Nacional). The candidate argued that the processing was necessary for his legitimate interest to communicate with the electorate, explain his platform and ask for their vote. The Court considered that the candidate could lawfully use the email addresses of all members of the association for his legitimate interest. The Court pointed out that the application form for the professional association stated that contact information of members will be provided to other members, the governing bodies and to third parties with a legitimate interest.
Publishing in an archive of a real estate website the selling price of a house that is not on the market anymore **Source:** Data Protection Authority, Denmark (June 17, 2014)[104]	The Data Protection Authority from Denmark rejected a complaint from a data subject that required a real estate website to remove information regarding the data subject's property previous listing on the market. The DPA held that information about the property address, asking price, year of construction, size and type of construction is personal data, but it is non-sensitive personal data. Even if not published on the real estate website, this information is available for all to have access to pursuant to the Land Registration Act. The DPA also argued that the website has a legitimate interest in processing the information: the purchase and sale of housing as an essential investment for a person, with information on prices and price trends being an important criterion for such an investment decision. The DPA underlined that the property information is available in the archive section of the website and the website clearly states that the property is no longer on the market and that the previous price should not be seen as reflecting the property's current market value.
Video surveillance of a swimming pool area **Source:** Data Protection Authority,	The Data Protection Authority of Norway (DPA) undertook an inspection into the use of video surveillance monitoring by a swimming facility pursuant to the Personal Data Act ("Act"). The swimming pool has 28 cameras which were located in wall corners and underwater in the general swimming pool, the separate family area; and the adult wellness area. The purpose for surveillance included monitoring of perimeter protection, and security and the prevention and investigation into unwanted sexual conduct. Article 8(f) of the Act provides that personal data may be processed if there is a legitimate interest for processing. The DPA reasoned that the swimming facility is permitted to use video surveillance if the need for surveillance it is

[103] https://nymity-my.sharepoint.com/Users/grabiuta/Downloads/36fe8dad-b7ec-48d2-8c45-b8db9f531736.pdf
[104] 2014. Datatilsynet, Denmark - Processing of Personal Data on a Real Estate Website. Retrieved from https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/behandling-af-personoplysninger-paa-boligadk/ .

Processing activity & Source	Summary
Norway, July 8, 2015.[105]	greater than violation of privacy of the employees, customer and visitors. It found that the video surveillance footage to monitor swimming pool visitors in the general and family designated swimming area was permissible for the purposes of security and the prevention of unwanted sexual conduct (protecting human life and health is a legitimate interest). However, video surveillance had to be removed from the adult designated area since the safety of the visitors does not outweigh their privacy (the adult area offers a quiet place to relax, serves alcohol and access to the area is controlled through the purchase of a wristband).
Recording for historical research purposes **Source:** Data Protection Authority in Greece, October 17, 2016.[106]	An individual had asked the data protection authority in Greece ("DPA") if he can use personal data previously collected on the inhabitants of a village in a genealogy book, including name, age, marriage information, profession and aliases. It was found that historical research is a legitimate interest that can take precedence over individual rights and freedoms (particularly since the individuals had previously provided the data for another purpose); and the author can use the personal data if, before the book is published, data subjects are informed of the processing of their personal data, and the DPA is notified of the personal data file.
Recording of employee misconduct Data Protection Commissioner of Ireland, Annual Report 2016, Case Study 10[107]	In Case Study 10/2016, the DPC confirmed that no breach of the Data Protection Acts had occurred when photos and audio of a sleeping employee were taken by the employee's supervisor. The photos and audio were passed to the employer for disciplinary purposes; and relied on by the employer as part of disciplinary proceedings. This ultimately led to the dismissal of the employee. The DPC ruled that the processing was proportionate and that the legitimate interests of the data controller outweighed the employee's right to protection of his personal data. The DPC considered the circumstances of the complaint and in particular, the vulnerability of the clients involved; and nature of the employee's duties.
	Two Greek insurance companies requested a DPA-exemption from obtaining consent to transfer policyholder, employee, and client data to complete a

[105] Datatilsynet - Decision 15-00209-10 - Cameras in Swimming Pool. Retrieved from https://www.datatilsynet.no/globalassets/global/regelverk-skjema/avgjorelser-datatilsynet/tilsynsrapporter/2015/15-00209-10-kontrollrapport-ankerskogen.pdf.
[106] https://www.personuvernd.is/efst-a-baugi/urskurdir-og-alit/2015/greinar/nr/2004
[107] https://www.dataprotection.ie/documents/annualreports/AnnualReport16.pdf

Processing activity & Source	Summary
Providing personal data as part of a merger DPA Greece – Order 131, 2017.[108]	merger. They argued that consent is not required since all data of the assignee will automatically become an asset of assignor upon completion of the merger and notice of the merger can be made through a press announcement in 2 national newspapers, and postings on the companies' official websites. The DPA noted that article 5 of the Law on Processing of Personal Data permits personal data processing without data subject consent if absolutely necessary to fulfill a legitimate interest of the controller or a third party and granted the exemption.
Processing customer data between car dealerships Data Protection Commissioner Ireland, Annual Report 2011, Case Study 6[109]	The DPC determined that when a company purchases a business from a liquidator, they usually buy the customer data as well. In these cases, customer data can be legitimately used if it is for the same purposes as the previous owner had used them.
Debt Collection DPA Bulgaria, Decision No. ZH-67/2014[110]	The Bulgarian DPA issued a decision regarding a complaint that a Bank transferred personal information to a third party without authorization. The complainant was a customer of the bank and had signed a contract with the Bank for the issuance of a credit card in his name. He received a letter from the Bank notifying the Complainant that the outstanding debt owed on his credit card was being transferred to a debt collection agency and complained to the DPA that the Bank provided his personal and financial information to the agency without his express permission. The DPA considered that under article 4 of the Data Protection Act, a data controller may process personal information only when at least one of the following conditions are met:

[108] DPA Greece, Order 131, 2017, http://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2017&_piref33_15473_33_15453_15453.arithmosApofasis=&_piref33_15473_33_15453_15453.thematikiEnotita=-1&_piref33_15473_33_15453_15453.ananeosi=Renewal

[109] Twenty-Third Annual Report of the Data Protection Commissioner 2011. Retrieved from https://www.dataprotection.ie/documents/annualreports/AnnualReport2011.pdf.

[110] Commission for Data Protection, Bulgaria - Decision No. ZH-67/2014 - Decision on Complaint Regarding Debt Collection. Retrieved from https://www.cpdp.bg/index.php?p=element_view&aid=1346.

Processing activity & Source	Summary
	the data subject has given their explicit consent, or processing is necessary for the execution of a contract to which the data subject is a part, or the legitimate interests of the data controller or third party to whom the data are disclosed. The DPA found that in this case, the Bank's debt-collection actions are admissible under the Act because the Bank: is a data controller as defined under article 3 has a legitimate interest in collecting the debt owed by the Complainant as a result of his credit card transactions and has a legal right to share his personal data with the Bank's sub-contractor because of the terms and conditions in the Bank's contract with the Complainant.
Using audio recording and photographs of data subjects Data Protection Commissioner of Ireland, 2016 Annual Report, Case Study 10[111]	The Irish DPC examined received a complaint from a former employee of a residential care home who claimed that photographic evidence and an audio recording of them were used in a disciplinary case resulting in their dismissal. In reviewing the information, the DPC considered the vulnerability of the clients involved and the nature of the complainants duties and formed the view that no breach of the law had occurred. The DPC considered that the processing of the complainant's data and the subsequent disclosure of these to the employer was necessary for the purposes of the legitimate interests pursued by the data controller. In balancing these interests against the fundamental rights and freedoms of the data subjects, the DPC considered that processing of personal data was limited in nature and scope and there had been limited further disclosure. It considered that in the circumstances, the processing was proportionate and that the legitimate interests of the data controller and the legitimate interests of the third parties (a vulnerable population of clients of a residential home) outweighed the complainant's right to protection of their personal data.
Processing biometric data to monitor employee attendance and access	The Portuguese DPA reviewed a company's request for authorization to process biometrics pursuant to the Data Protection Law ("Law"). The company sought approval to process employee's biometric data for attendance and access control purposes including: name, employee number, time or employment, department, section, date and time of entry, date and time of departure and a template of the fingerprint (which resulted from the interpretation algorithm of pyshiometric pints with no possibility of reconstruction of the biometric data). Under article 6(e) of the Law. The collection of employee's fingerprints to monitor attendance and access was

[111] 2016 Annual Report of the Data Protection Commissioner of Ireland. Retrieved from https://www.dataprotection.ie/documents/annualreports/AnnualReport16.pdf.

Processing activity & Source	Summary
DPA Portugal – Authorization No. 13457, 2017[112]	authorized by the DPA. It found that the processing is done under the legitimate interest of the employer (monitoring of employee attendance and access) and that once collected, the fingerprints are converted into a template that does not allow its reconstruction. Before implementing the system. the company was instructed to notify employees (required under Article 10 of the Law) and be able to accommodate any objections. The
Conducting customer surveys Data Protection Authority, Iceland, October 22, 2015[113]	The Data Protection Authority of Iceland (DPA) investigated a complaint pursuant to Act 77/2000 on Data Protection (the "Act") regarding a customer survey. A customer complained to the DPA that a telecom had given his number to a company in order to conduct a survey. The telecom indicated that they only shared anonymous customer contract details and the customer's phone number with their consulting company. The consulting company indicated that the shortlist of randomly selected "active" customers used for the survey was deleted after use and responses of individual customers to the survey could not be traced. The DPA found that the processing was permissible on the basis of the data controller's legitimate interests pursuant to Article 8 of the Act. (Note, ultimately, the DPA found the processing unlawful because the controller failed to have a written contract in place with the company conducting the surveys (i.e. the processor) which was required under Article 13 of the Act.
Sharing name and contact information of candidates for potential jobs in order to negotiate employment contracts DPA Slovenia – Opinion 0712-1-2015-2141[114]	The Information Commissioner of Slovenia issued an opinion on processing employee and potential employee personal data. A recruitment firm asked if it is necessary for employers to send notices of lists of suitable candidates for a job opening by mail only (employers did not want to communicate contact information by email due to privacy concerns). Submitting employment contracts to the Health Information Institute was necessary to obtain compulsory health insurance. The DPA found that sharing contact information of potential candidates with recruiting firms is necessary and appropriate for conducting contract negotiations; it would be a legitimate interest of an unemployed person to find a job as soon as possible and email communications would result in a faster path to employment.
Collecting biometric data	The DPC investigated a compliant in which the complainant

[112] DPA Portugal, Authorization No. 13457 2017 – Seara, S.A.. Retrieved from https://www.cnpd.pt/bin/decisoes/Aut/10_13457_2017.pdf
[113] DPA Iceland - Case No. 2015-1012 - Disclosure of Personal Data for Survey Purposes. Retrieved from http://www.personuvernd.is/efst-a-baugi/urskurdir-og-alit/2015/greinar/nr/2004
[114] DPA Slovenia - Opinion 0712-1-2015-2141 - Personal Data of Employees and Candidates. Retrieved from https://www.ip-rs.si/vop/osebni-podatki-delavcev-in-kandidatov-2633/

Processing activity & Source	Summary
and passport identification for security purposes Data Protection Commissioner o Ireland, Annual Report 2016, Case Study 9[115]	stated that in the course of attending a data centre for work-related purposes the company had collected their biometric data without their consent and had also retained their passport until they had departed from the data centre. In relation to the obtaining and processing of the complainant's biometric data, the DPC found that the data controller had a legitimate interest under Section 2A(1)(d) of the Acts in implementing appropriate security procedures for the purposes of safeguarding the security of data centre, in particular for the purposes of regulating and controlling access by third parties to the data centre. Given that the biometric data was used solely for the purposes of access at the data centre, it was not transferred to any other party and was deleted in its entirety at the data subject's request upon departing the data centre, the DPC's view was that this did not amount to potential prejudice that outweighed the legitimate interests of the data controller in protecting the integrity of the data centre and preventing unauthorised access to it. **Comment:** Under the GDPR, since biometric data was included on the list of special categories of data in Article 9 GDPR, the outcome of this case could be different, unless the Irish law will provide for specific grounds of processing biometric data.
Call recordings for purposes of documenting contractual agreements DPA Sweden, Decisions 120-2016 and 121-2016[116]	The Swedish DPA investigated how two telecom companies handled recordings of customer calls to their call centers. It examined the practice of recording calls at random for the purposes of employee training and quality control. It further examined the practice of recording for the purposes of documenting the agreement by the customer for a contract. Both companies were ordered to cease processing customer's data through the random recording of phone calls or better inform the customer of the purposes of processing. One company was further ordered to better notify customers of recording for contractual purposes. **Recordings for contractual purposes:** For company A, it was found that the recordings were stored for 5 years and were saved using the customer's telephone number or social security number. The company had a legitimate interest in the recordings that outweighed the customer's interests. While the recordings were not necessary for the conclusion of the contract, they document an agreement by the customer to a contract and the customers were given the ability to object to the recording. For Company B, it was also found that the company had a legitimate interest in the recordings and customers were provided with an ability to object to the recordings. For Company A it was found that if the customer's consented to the recordings they were not provided sufficient information to advise them how to exercise

[115] 2016 Annual Report of the Data Protection Commissioner of Ireland. Retrieved from https://www.dataprotection.ie/documents/annualreports/AnnualReport16.pdf.
[116] https://www.datainspektionen.se/Documents/beslut/2016-05-12-telia.pdf

Processing activity & Source	Summary
	their rights and for Company they were not provided any further information about the processing of their data. Both companies were ordered to better inform callers of these recordings pursuant to sections 23 and 25 of the Data Protection Act.