# The Much-Awaited Guideline on the Processing of Special Categories of Personal Data Has Been Published!

**14 March 2025**

As is known, significant amendments were made to the Turkish Data Protection Law (**DP Law**) last March -particularly regarding its provisions on processing of special categories of personal data and transferring personal data abroad- to align the legislation with the European Union General Data Protection Regulation (**GDPR**).

*(You can access our infographic note on the amendments introduced by the DP Law here)*

Following these developments, many were expecting the Personal Data Protection Authority (**Authority**) to publish guidance on both issues to address any possible doubts that may arise afterwards. Indeed, the Guideline on Transferring Personal Data Abroad was published on the 2nd of January.

*(We have published the points that attracted our attention in the Guideline on Transferring Personal Data Abroad here).*

This time around, the Authority published its second expected guideline regarding the amendments: the Guideline on the Processing of Special Categories of Data (**Guideline**). We have gathered for you below the issues that are introduced for the first time in the Guideline and those we consider important.

## A. Clarifications on the Special Categories of Personal Data

DP Law listed the special categories of personal data on a *numerus clausus* basis (i.e., in a limited list), but didn't explain what they meant and how they should be interpreted. Although practitioners were consulting the Authority's decisions and other guidelines when assessing the scope of such data, there was no clear answer. This caused many uncertainties in practice.

The Guideline clarifies these uncertainties to some extent. Indeed, the meaning and scope of each category of sensitive personal data is described with references to the definitions made by the Turkish Language Association (**TDK**), the Court of Cassation, the Council of State, national and international legislation and various institutions.

Further explanations the Guideline provide for special categories of personal data are summarized as follows:

- **Explanations on Data Concerning Race and Ethnic Origin:** In practice, there were discussions on whether nationality data was included in this category. The Guideline ended these discussions once and for all.

The Guideline stated that since the concept of "*nationality*" is not listed under the DP Law -following the *numerus clausus* principle - this information cannot be considered as a special category of personal data.

Therefore, the Guideline clarifies that data processed by the data controller such as "*foreign citizen*", "*not a citizen of the Republic of Türkiye*", "*other*" are not special categories of personal data. Accordingly, information such as country code and nationality in various documents (e.g., old-type passports, driver's licenses, identity cards or student IDs, and workplace IDs) are not considered special categories of personal data either.

- **Explanations on Data Concerning Political Opinion:** Until now, this term has neither been defined in DP Law nor in the GDPR. The Guideline provides explanations on this matter.

  Information about a person's political party membership, political opinion or apolitical views, as well as a person's socio-political behavior and attitude are considered political opinion data. Hence, information about the political party a person supports in surveys conducted for public opinion research on elections is also considered a special category of personal data in the Guideline.

  The Guideline also refers to the GDPR and states that if it is necessary to process people's political opinions for the functionality of the democratic system during elections, political parties may process special categories of personal data for public interest by taking appropriate measures.

- **Explanations on Data Concerning Philosophical Belief, Religion, Religious Sect or Other Belief:** "*Not having any beliefs*" is also included under this category. On the other hand, the Guideline states that belief must reach a certain level of credibility, seriousness, commitment and importance.

- **Explanations on Data About Attire and Clothing:** The Guideline states the purpose for including these data under special categories is to prevent discrimination and violation of rights and emphasizes that this purpose should be interpreted on a case-by-case basis.

  As part of its explanations, the Guideline refers to a Council of State decision on a request for the annulment of a by-law article, filed by a government official who had been subjected to a disciplinary penalty for "*wearing jeans*" and "*growing a beard*".

  The Guideline appears to merely highlight the Council of State's following statements in its decision: **(i)** legal practices prescribing sanctions that may make people feel inferior due to their inherent or acquired distinctive characteristics would legitimize inequality and discrimination, and **(ii)** individuals have the freedom to express themselves through their physical appearance, such as the length of their beards.

In its decision, the Council of State assesses that the phrase *"...Beards must be shaved every day, and beards cannot be grown..."* in the relevant by-law article concerning male personnel may potentially undermine the principle of equality, lead to discrimination, and is not compatible with the requirements of a democratic social order.

> **Our comment:** As data about attire and clothing is not included in international regulations on the protection of personal data, it was initially unclear how it would be interpreted in practice. The Guideline clarifies that, this data is protected as a special category of personal data under DP Law to prevent discrimination based on appearance. However, since it also states that such data should be evaluated on a case-by-case basis, discussions on its interpretation may still arise in practice.

- **Explanations on Data Concerning Health and Sexual Life:** Based on the definition of "*personal health data*" in DP Law, the Guideline states that health data includes both the state of being healthy and data indicating or identifying the possibility of illness.

  In this context, results of examinations and preliminary diagnosis, diagnosis, and treatment information enabling determination of physical, mental, and social status are considered as special categories of personal data. In addition, the Guideline considers the processing of "*blood type information*" included in certain documents (e.g., old-type passports, driver's licenses, identity cards, and workplace IDs) as the processing of special categories of personal data.

- **Explanations on Data Concerning Criminal Convictions and Security Measures:** The Guideline states that final convictions constituting the content of criminal records, as well as the security measures under Article 53 and subsequent provisions of the Turkish Criminal Code, may be considered special categories of personal data.

  As mentioned in the example in the Guideline, processing the convictions in the criminal record (e.g., imprisonment sentence, decision to release on probation, conviction for a judicial fine, and revocation of the driver's license) is considered processing special categories of personal data.

  > **Our Comment:** Based on the Guideline's example above, there is uncertainty regarding how to evaluate clean criminal records – that is, cases where there is no conviction or security measure recorded.
  >
  > However, statements made by Authority officials in public meetings were understood to mean that a clean criminal record would not be considered a special category of personal data. Although practitioners had hoped the Guideline would provide clarity on this issue, this statement unfortunately did not meet the expectations.

- **Explanations Regarding Biometric Data:** The Guideline defines biometric data as *"data that individuals cannot forget, generally remain unchanged throughout their lifetime, and*

*are effortlessly possessed without any intervention".* It provides examples of physiological and behavioral biometric data.

The Guideline states that photographs, including biometric ones, cannot be directly considered as biometric data. These data are considered special categories of personal data, only in cases where they are processed by specific technical means that allow a person to be uniquely identified or authenticated.

> **Our Comment:** First, the Guideline states that a photograph will be considered biometric data "*if it is processed by a specific technique*", then further establish that a data must "*have the ability to identify or verify the person*" to be considered as biometric data.
>
> Therefore, there is an uncertainty as to whether these two criteria will be sought together or separately, and there seems to be a contradiction between the two statements.
>
> However, when the Guideline and previous Authority decisions are considered, in our view, it seems likely that Authority will assess both criteria together and that biometric photographs will not be considered a special category of personal data unless they are processed for identity verification.

- **Explanations Regarding Genetic Data:** Referring to the GDPR, the Guideline defines "*genetic data*" as "*personal data relating to the inherited or acquired genetic characteristics of individuals resulting from the biological analysis of a sample taken from the individual*".

The Guideline highlights that a genetic sample, by itself, is not considered a special category of personal data. It states that information obtained from this sample through various processes is regarded as genetic data. For example, it explains that analyzing a sample obtained ten years ago using today's technology to assess whether the sample owner's children may carry certain diseases would be considered genetic data.

In addition, it emphasizes that genetic data may be accessed at any time from DNA/RNA samples, under proper storage conditions.

Since information can be obtained from any tissue or material sent to a laboratory for research or diagnostic purposes, the Guideline emphasizes that data controllers collecting biological samples must implement the necessary technical and administrative measures to ensure their security from the moment the samples are obtained.

> **Our Comment:** In practice, since genetic data can be easily obtained from a blood sample, whether a blood sample alone could be considered as genetic data was uncertain. Based on the Authority's decisions and the GDPR practice, we were in the opinion that a blood sample alone would not be "*personal data*".

The Guideline explicitly identifies *"information resulting from the analysis of a sample obtained from the subject"* as a special category of personal data. However, it is unclear whether the "*necessary technical and administrative measures*" required for such samples under the Guideline refer to the specific measures prescribed for special categories of personal data.

In this context, there may be discussions on whether a data controller, who fails to implement security measures and causes the relevant sample to be obtained by third parties, will be penalized by the Authority for failure to ensure sufficient protection for special categories of personal data; as these samples should not be considered special categories of personal data at the stage of obtaining and storing without analysis.

However, since it is possible to obtain genetic data from these samples due to their nature, it can, in any case, be stated that a cautious approach should be taken, and high-level measures should be implemented to ensure their protection.

## B. Clarifications on the Legal Bases for Processing Special Categories of Personal Data

DP Law provides limited legal bases for processing special categories of personal data. In addition to what has been stated in previous Authority decisions or guidelines, we observe that the Guideline provides more clarity and details the implementation for some of these legal bases. These are summarized as follows:

- **Additional Clarifications for 'Necessity for the Establishment, Exercise, or Protection of Any Right' Legal Basis:** The Guideline states that "necessity" should be identified for each data processing activity, and the scope of the establishment, performance, and protection of a right should be determined.

  In addition, the Guideline explains that special categories of personal data may also be processed for the establishment, performance, or protection of a *third party's rights*. For example, employers may rely on this legal basis where it is necessary to process certain data of spouse and children (e.g., disability or health information) for salary payments of an employee.

- **Additional Clarifications for 'Necessity for the Protection of Public Health, Preventive Medicine, Medical Diagnosis, Treatment and Care Services, as well as the Planning, Management, and Financing of Healthcare by Persons Under a Confidentiality Obligation or Authorized Institutions and Organizations' Legal Basis:** Essentially, the Guideline clarifies the scope of this legal basis.

  The Guideline states that "*authorized institutions and organizations*" cover not only public institutions and organizations, but also individuals and private legal entities providing healthcare services.

Referring to the GDPR, it states that public health should be interpreted as "*all aspects of health, including illness and disability, health care needs, resources allocated to health care, provision and universal access to health care, and determinants that have an impact on health expenditure and financing*".

For example, this legal basis is considered applicable to family physicians' monitoring of mandatory childhood vaccinations, which is required by state policy.

- **Additional Clarifications for 'Necessity for Compliance with Legal Obligations in Employment, Occupational Health and Safety, Social Security, Social Services, and Social Assistance' Legal Basis:** The Guideline clarifies the scope of this legal basis.

  The Guideline states that "*necessity*" does not necessarily have to derive from the law; it may arise from an explicitly stipulated obligation, a by-law, directive, communiqué, or contract.

  The Guideline considers the processing of special categories of personal data to be lawful if institutions and organizations with legal obligations related to occupational health and safety, social services, and social assistance cannot fulfill their legal obligations (e.g., determining needs and coordinating aid) by other means.

  It also deems it lawful for a worker to undergo a different medical examination required by the nature of the job under a collective labor agreement. Additionally, the Guideline includes definitions of concepts such as employment, occupational health, and safety.

  At the same time, the Guideline highlights the provision in the Turkish Code of Obligations No. 6098, which states: "*The employer may use personal data belonging to the employee only to the extent that it is related to the employee's suitability for the job or necessary for the performance of the employment contract. Special provisions of other laws are reserved*" -thus emphasizing its applicability to all employment relationships.

  > **Our Comment:** The Guideline treats the provision referenced in the Turkish Code of Obligations as a legal obligation for employers. As a result, it can be argued that employers may now process special categories of personal data by claiming that it is necessary for the job itself. For instance, health data included in medical reports obtained during hiring or in sick leave reports.

## C. Actions to be taken by Data Controllers for Compliance with the Law

DP Law requires data controllers to implement adequate measures determined by the Authority, with these measures being detailed in an Authority decision. The Guideline repeats these measures and emphasizes that data controllers should take the following steps immediately:

- Legal bases under personal data processing inventory should be updated for processing of special categories of personal data, and compliance with Data Controllers' Registry (**VERBIS**) processes should be prioritized.
- Since new legal bases have become available after the DP Law amendment, explicit consent processes should be reorganized, and privacy notices should be updated.

  **Our comment:** In particular, since employees' health data, which was previously processed based on explicit consent, can now be processed under the employment-related legal basis; privacy notices and explicit consent forms will need to be revised accordingly.

- Personal data storage and destruction policies should be updated according to applicable legislation.
- Data security measures specified in the legislation, guidelines, and Authority decisions must be implemented.

Kind regards,


Bora Yazıcıoğlu
bora@yazicioglulegal.com

Kübra İslamoğlu Bayer
kubra@yazicioglulegal.com

Aslı Rabia Savaş
asli@yazicioglulegal.com

Doğa Satı
doga@yazicioglulegal.com