

# Data Protection Update for Poland

Article By:

Magdalena Gad-Nowak

---

## Updated Black List of Processing Operations Requiring DPIA

On July 8, 2019 the updated list of operations requiring a data protection impact assessment (DPIA) was published in the official gazette of the Republic of Poland. The “black list” was updated by the Polish data protection authority, after the European Data Protection Board (EDPB) raised its objections to the original draft published by the Polish regulator on August 17, 2018. According to [the EDPB’s opinion 17/2018](#), the original “black list” could have led to inconsistent application of the requirement for a DPIA and, therefore, should be subject to modifications.

As a result of the EDPB opinion, the Polish supervisory authority has recently made changes to the Polish “black list” of processing operations requiring a DPIA:

- The list now includes an explicit reservation that its nature is non-exhaustive (a feature it previously lacked) and that it merely aims to help the controllers to better understand the criteria/types of processing operations which might trigger the DPIA requirement. As such, the controllers are still obliged to conduct proper risk assessment and manage such risks accordingly.
- There is now a clear reference to the Working Group 29 Guidelines (WP248) on data protection impact assessment (as endorsed by the EDPB), on which it has based, and emphasizes that, in most cases, only the processing meeting two of the criteria listed therein would require a DPIA (a reservation it previously lacked).
- The list now contains the processing of biometric data, either for the purpose of uniquely identifying a natural person or for access control purposes (the original “black list” did not include it, to which the EDPB objected).
- The list now enumerates the processing of genetic data (e.g. hospitals/laboratories/companies offering genetic diagnostics, e.g. DNA tests).
- The list has expanded by adding the processing of location data (e.g. applications and devices using IoT, data processed in connection with remote working or processing of employees’ GPS/location data).

---

## License Plate Number Is Not Personal Data

On June 28, 2019 the Supreme Administrative Court of Poland (*Naczelny Sąd Administracyjny*) ruled that license plate numbers typed into Warsaw parking meters are not personal data.

The court reasoned that at the time the license plate number is typed on the parking meter it is impossible to identify the person entering the number. The ruling caused a tantrum among lawyers, who argue that license plate numbers are personal data just as much as IP address and, as such, should be deleted by the meters once the ticket confirming that the parking payment has been made is printed. Any storage of this data in the memory of the meter and the municipal data base (especially for eight years, as in the case at hand) is unjustified and unreasonable. The city of Warsaw argued that it is virtually impossible to identify the driver of the vehicle parking in the city because the city authorities generally lack access to CEPiK (Central Evidence of Vehicles and Drivers). Therefore they are unable to identify the driver. And even if they had access to CEPiK (which may be the case at the stage of enforcing the unpaid parking fee), it might be impossible to track the location of the actual driver because CEPiK contains information on only the vehicle owners. Drivers are not always owners – one vehicle may be used by two or more persons. Oftentimes, vehicles are registered under the names of more than one entity. Thus it is difficult to tie the vehicle to one specific person without extraordinary efforts. The license plate number identifies the vehicle and not the person.

It is worth mentioning that, five years ago, a regional administrative court (whose ruling is still in force and binding) found quite the opposite – that a license plate number *is* personal data. As a result, these two rulings of two courts are entirely contradictory. This causes significant legal chaos and is more difficult to understand as personalized license plate numbers (comprising the name or last name of the owner of the vehicle) become more and more popular.

Moreover, the most recent ruling of the NSA seems to be against the common EU-wide trend of increasing levels of data protection (vide GDPR). The ruling of the Polish court clashes in particular with the approach to license plate numbers as personal data represented by the UK and Germany.

## Data Breach Manual

On May 30, 2019 the Polish supervisory authority published [detailed guidelines \(in Polish\)](#) on the duties of controllers in connection with data breaches under the GDPR.

The major highlights of the UODO's manual (which generally mimics the WP 29 recommendations in this respect) include:

- Controllers are expected to design and implement solid breach and assessment procedures that contain, in particular, the list of potential threats and breaches that may occur at the given controller, the description of all stages of managing the breach (from detection to elimination) and the personnel's code of conduct in case a data breach occurs
- Processors shall notify the controllers of the identified breaches without undue delay (as soon as possible) –this stems directly from article 33 item 2 of the GDPR
- Controllers who assess that the regulator should not be notified of the given breach should record such decision and the underlying justification in the internal data breach register

- Responsiveness to the regulator's queries is expected of the controllers – failure to respond to the regulator's requests for information may trigger fines
- Data breach notifications can be made either electronically by filing in the [appropriate form online](#) or via regular mail ([by filling in this form](#))
- Unlawful and unauthorized loss or disclosure or access to the name, surname and PESEL number will always cause high risk to the rights and freedoms of natural persons and, as such, will always be subject to notification to UODO and the data subjects

The manual points out also the major mistakes that are regularly made by controllers when notifying of data breaches, these being:

- Incompleteness of information provided by the controller required under article 33.3 of the GDPR (e.g. lack of description of the nature of the breach or the possible consequences thereof, lack of description of measures implemented by the controller in order to mitigate the consequences of the breach)
- Lack of reliable description – descriptions are laconic and unreliable, requiring the regulator to further inquire about the breach (e.g. "document lost" without specifying what document and what data was lost)
- Lack of attention to details, routine, careless notifications which oftentimes contain information regarding different data breaches
- Notifications are made by processors, as opposed to controllers, who are obliged to notify of data breaches which occurred in connection with the entrustment of data processing

The guidelines also touch upon the data breach notification obligations arising under other legal acts. More on this can be found in our post [Personal Data Breach Notification Obligations Arise from Various Sources, not Only the GDPR](#).

© Copyright 2024 Squire Patton Boggs (US) LLP

---

National Law Review, Volumess IX, Number 202

Source URL: <https://www.natlawreview.com/article/data-protection-update-poland>