

# Co wolno ochroniarzowi?

■ **Czy pracownik ochrony w zakładzie wodociągowym albo oczyszczalni ścieków ma prawo legitymować osoby przebywające na terenie ochranianego obiektu i pozyskiwać na te potrzeby ich dane osobowe?**

Uprawnienia pracownika ochrony do legitymowania oraz pozyskiwania danych osobowych ludzi przebywających lub wchodzących na teren chronionego obiektu wynikają wprost ze szczególnych przepisów prawa. Zezwalają one m.in. na pozyskiwanie i spisywanie numerów dowodów osobistych osób legitymowanych, nie uprawniając zaś do zbierania takich ich danych jak imię ojca.

### Na mocy szczególnych przepisów

Zgodnie z art. 5 Ustawy z 22 sierpnia 1997 r. o ochronie osób i mienia (DzU z 2005 r. nr 145, poz. 1221), obszary, obiekty i urządzenia ważne m.in. dla bezpieczeństwa publicznego czy interesów państwa podlegają obowiązkowej ochronie, która może być realizowana przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne. Do obiektów mających duże znaczenie dla funkcjonowania aglomeracji miejskich, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, zalicza się m.in. elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków. Zatem to szczególne przepisy prawa zezwalają, by w zakładzie wodociągowym czy oczyszczalni ścieków działała formacja ochronna.

Jej uprawnienia określono w rozdziale 6 ustawy oraz w Rozporządzeniu Rady Ministrów z 18 listopada 1998 r. w sprawie szczegółowego trybu działań pracowników ochrony, podejmowanych wobec osób znajdujących się w granicach chronionych obiektów i obszarów (DzU nr 144, poz. 933). Zgodnie z art. 36 ustawy, pracownik ochrony, przy wykonywaniu swoich zadań, ma prawo m.in. do ustalania uprawnień do przebywania na obszarach lub w obiektach chronionych oraz legitymowania osób w celu określenia ich tożsamości. Z kolei §2 ww. rozporządzenia stanowi, że ochroniarz może spraw-

dzić, czy osoba posiada przepustkę, identyfikator albo inny dokument uprawniający do przebywania na obszarze lub w obiekcie chronionym, wystawiony przez osobę nim zarządzającą, porównać okazany dokument z określonym wzorem oraz zbadać ten dokument pod względem zarówno zgodności danych personalnych w nim zawartych z tożsamością osoby, jak i terminu jego ważności. Ustalenia uprawnień do przebywania na danym obszarze czy w obiekcie pracownik ochrony może dokonać także na podstawie ustnego lub pisemnego upoważnienia, wydanego przez zarządzającego tym obiektem lub obszarem.

Ochroniarz może sprawdzić, czy osoba posiada przepustkę, identyfikator albo inny dokument uprawniający do przebywania na obszarze lub w obiekcie chronionym, wystawiony przez osobę nim zarządzającą, porównać okazany dokument z określonym wzorem oraz zbadać ten dokument pod względem zarówno zgodności danych personalnych w nim zawartych z tożsamością osoby, jak i terminu jego ważności.

Przed rozpoczęciem legitymowania ochroniarz powinien m.in. podać podstawę prawną i przyczynę tej czynności (§3). Natomiast tożsamość osoby legitymowanej ustala się na podstawie np. dowodu osobistego, paszportu lub innych dokumentów potwierdzających tożsamość, zaopatrzonych w fotografię i adres zamieszkania tego człowieka (§4 ust. 2). Z czynności legitymowania pracownik ochrony sporządza notatkę służbową, zawierającą dane personalne sprawdzanej osoby, wskazanie rodzaju dokumentu oraz jego numeru i serii, a także czasu, miejsca i przyczyny legitymowania (§6). Oznacza to, że oprócz wymienionych informacji pracownik ochrony nie powinien spisywać żadnych innych danych zawartych w dokumentach, na podstawie których ustala tożsamość osoby.

Dodatkowo, biorąc pod uwagę przepisy Ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych, należy wskazać, że jej art. 26 zobowiązuje administratorów do zbierania danych osobowych dla oznaczonych, zgodnych z prawem celów i niepoddawania ich dalszemu przetwarzaniu, niezgodnemu z tymi celami. Są oni ponadto zobowiązani zapewnić, aby informacje te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (pkt 3).

### Adekwatność danych

Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w którym dane są przez niego przetwarzane (wyrok Wojewódzkiego Sądu Administracyjnego z 1 grudnia 2005 r. – sygn. akt II SA/Wa 917/2005). Zasada celowości przetwarzania danych osobowych oznacza zaś, że administrator danych może je wykorzystywać jedynie w celu realizacji przypisanych mu zadań lub kompetencji. Przy czym cel przetwarzania danych osobowych nie jest wynikiem arbitralnej decyzji, oderwanym od okoliczności przetwarzania, co oznacza, że ustalając cel, należy odwołać się do kontekstu przetwarzania. Swoim rodzajem oraz treścią dane osobowe nie powinny zatem wykraczać poza potrzeby wynikające z celu ich przetwarzania.

Reasumując, należy uznać, że skoro przepisy szczególne w stosunku do ustawy o ochronie danych osobowych wprost określają, do przetwarzania jakich danych osobowych są uprawnieni pracownicy ochrony, to nie powinni oni pozyskiwać danych wykraczających poza ten zakres.

**dr Wojciech Rafał Wiewiórowski**  
Generalny Inspektor Ochrony  
Danych Osobowych

*Tytuł i śródtytuły od redakcji*