Parsing ICO Storage and Access Guidance Exceptions

By **Jonathan Wright and Ashley Webber** (July 16, 2026)

Jonathan Wright

Ashley Webber

On April 29, the U.K. Information Commissioner's Office published the final updated version of its guidance on storage and access technologies, such as cookies, pixels and web storage.[1]

The guidance takes into consideration the requirements of the Privacy and Electronic Communications Regulations, the General Data Protection Regulation and the latest changes introduced to U.K. data protection law by the Data (Use and Access) Act.

Updating the guidance forms part of the ICO's online tracking strategy and follows two public consultations: The first consultation regards general updates to the guidance, while the second consultation focuses on the changes to privacy and electronic communications made by the DUAA.

This article focuses on the DUAA's changes, specifically the new exceptions to the requirement to obtain consent for the use of technologies, and what these will mean for businesses.

The guidance sets out the key obligations for organizations when using technologies, such as when and how to obtain consent, and what information individuals must be provided with about the use of technologies.

Much of this information was in the ICO's previous version of the guidance, but the new guidance has introduced further detail on certain points and includes new practical examples. Most notably, as we will discuss here, the updated guidance considers the changes to the consent requirements for using technologies under the privacy and electronics communications regulations introduced by the DUAA.

Under these regulations, consent is required to use any technologies, unless they are used for very limited and specific purposes. The DUAA introduced three new exceptions to this rule: the statistical purposes exception, the appearance exception and the emergency assistance exception.

Below is a summary of each of these exceptions and key considerations for implementing each exception as detailed in the guidance.

Statistical Purposes Exception

Under this exception, an organization is not required to procure consent to store or access information using technologies if the sole purpose of the storage or access is to enable the organization to collect information for statistical purposes about:

- How a service is used, with a view to making improvements to the service; or
- How a website by means of which the service is provided is used, with a view to making improvements to the website.

To rely on this exception, an organization must still provide clear and comprehensive information regarding the purposes for which technologies are used, as well as simple and free means to object to their use.

This exception is about the creation of aggregate statistical information regarding visitors to a service and the use of this information to improve the service, i.e., "essentially for analytics purposes," according to the ICO.

The ICO adds a caveat to this, by confirming the exception does not cover all analytics — it is about how the service is used and not about who uses the service. The exception is not to be relied upon to identify, track or monitor individuals, all of which would require user consent.

However, organizations will be able to rely on it for certain of their technologies currently categorized as analytics in their consent management platform.

To rely on the exception, the information collected should be statistical in nature. The ICO provides examples, such as how many individuals access the service, what they access and how long they access it for.

The ICO explains that improvements to the service may include understanding typical user journeys through the service to aid the decision as to how to organize the service or what content to produce more or less of, e.g., for a business-to-consumer retail business, how much detail to provide in the description of the product and where best to place that description.

The ICO acknowledges that such activity may involve the processing of personal data, and in such instances, the organization must comply with the GDPR and then aggregate the data. In line with the GDPR, personal data should not be stored for any longer than is necessary for aggregation purposes.

The ICO has prepared a table of nonexhaustive examples of activities that are likely to meet the exception, such as total visits to a service, user interactions with pages on a website, how users reached a service, information on page loading speeds, and bounce rates or exit pages. All such examples are clearly low risk from a privacy perspective and are common use cases for technologies categorized as "analytics" technologies in a consent management platform.

Regarding third-party analytics, the information collected by technologies should not be shared with a third party "except for the purpose of enabling that other person to assist with making improvements to the service or website." The ICO has interpreted this restriction to the exception to mean that a third-party analytics provider can be used by an organization, provided that:

- The provider acting on behalf of the organization, i.e., as a processor; and
- The information is only being used to help the organization improve its service, i.e., not the service of the third-party analytics provider.

As with existing notice requirements for technologies, an organization using a third-party analytics provider must inform users of its activities.[2]

Appearance Exception

Under this exception, an organization is not required to obtain consent to store or access information using technologies if the sole purpose of the storage or access is to enable the organization to:

- Adapt the way the organization's service appears or functions in line with the subscriber's or user's preferences; or
- Otherwise enhance the appearance or functionality of the website when displayed on, or accessed by, the subscriber's or user's device.

As with the above, to rely on this exception, an organization must still provide clear and comprehensive information regarding the purposes for using technologies, as well as a simple and free means to object.

The ICO highlights that this exception should not be relied upon to adapt the content displayed to a user on a service based on any known or inferred interests or behaviors of the user, e.g., using their profile to serve a specific ad.

Organizations will likely be able to rely on this exception for certain technologies currently categorized as functional technologies in their consent management platform. The ICO has prepared a table of nonexhaustive examples of activities that are likely to meet the exception, such as identifying the dimensions of a subscriber's or user's monitor or screen to enable the reconfiguration of a website to adapt to the monitor or screen, and remembering the language the subscriber or user selects.

Such examples are common use cases for technologies categorized as functional technologies in a consent management platform. The table also lists two examples of activities that would not meet the exception, i.e., changing the content displayed to a user based on known or inferred interests or behaviors about them, and online advertising. For both such examples, consent would still be required.

Emergency Assistance Exception

Under this exception, an organization is not required to procure consent to store or access information using technologies if the sole purpose of the storage or access is to identify the geographical position of the subscriber's or user's device to provide emergency assistance.

While similar to the existing exception for emergency calls under the privacy and electronics regulations — which allows the restrictions on the processing of location data to be removed when the user makes an emergency call — under this new exception, the information stored or accessed is not limited to location data.

Nor is the application of the exception limited to emergency calls, meaning it has a broader application, e.g., it could apply to other devices like tablets or smartwatches. To rely on this exception, an organization must either receive a communication from the subscriber or user seeking emergency assistance first or receive another indication that the subscriber or user needs emergency assistance.

As with the other exceptions, the ICO has prepared a table of nonexhaustive examples of

activities that are likely to meet the exception, such as personal safety alarms that use GPS features to send location information once the subscriber or user wearing them presses an emergency button.

The examples provided by the ICO have fairly narrow application, which is likely representative of the limited scope of this exception generally. Depending on the circumstances and functionalities, it may be that an organization could rely on this exception in an emergency situation involving employees, likely by leveraging company-owned devices. However, this will depend on the use case.

Simple Means of Objecting

As noted, to rely on either the exception for statistical purposes or the exception for appearance, an organization must provide users with "a simple means of objecting, free of charge, to the storage or access."

This term is not defined in the privacy and electronics regulations in the DUAA updates, so an organization looking to rely on either or both of these exceptions can implement this right to object by a means which is appropriate for its business.

In most instances, businesses will likely build the objection into the existing consent mechanism, toggling on the statistical/analytics or appearance/functionality technologies by default. However, this may prove challenging for businesses for two reasons.

First, if only certain technologies currently categorized as analytics could satisfy the statistical-purposes exception and/or only certain technologies currently categorized as functional could satisfy the appearance exception, the business would have to determine how best to present the technologies to the user — i.e., those that are being used on the basis of the relevant exception would require an opt-out, whereas those that are not would still require an opt-in.

This situation may result in an organization having to build more categories into its consent management platform.

Second, implementing the functionality to rely on these exceptions could prove challenging if the existing consent mechanism is also used in other countries in addition to the U.K. Importantly, as noted by the ICO, an organization must not rely solely on browser settings as an indication of whether a person does not object.

Conclusion

The guidance provides a thorough and practical overview of how an organization may seek to rely on any of the new exceptions introduced by the DUAA. The approach taken aligns with the previous version of the guidance with respect to determining, for example, what would be deemed a strictly necessary technology.

In practice, organizations generally find the ICO's tables of nonexhaustive use cases to be a useful reference point in categorizing technologies, so the new exceptions are a welcome development.

To the extent an organization sees benefits in the exceptions and wishes to explore relying on them, it should first look at the technologies it currently uses and confirm whether any such technologies could currently fall within the scope of the exceptions. In addition, an

organization could also consider technologies not currently used.

Once an organization has selected current or new technologies it wishes to use based on the relevant exceptions, it should consider how to operate such use, including, for example, implementing an opt-out and reviewing any applicable terms with technology providers. An organization relying on any exceptions should document the assessment and steps taken to comply with the relevant requirements.

As noted, updating the guidance forms part of the ICO's online tracking strategy. Compliance regarding the use of technologies has been a key focus of the ICO over recent years and will likely remain so for the foreseeable future.

Organizations should therefore continue to consider this a key area of data privacy compliance while seeking to leverage the new exceptions provided under the DUAA, where possible.

Jonathan Wright is a partner and Ashley Webber is an associate at Hunton Andrews Kurth LLP.

[1] https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/.

[2] Schedule 12 of the Data (Use and Access) Act 2025.