Register ID: 092682012915-24

PostEurop Position Paper on ePrivacy

Brussels, 21 December 2018,

PostEurop represents national postal operators across Europe. Its members take data protection extremely seriously. For centuries, the posts have been trusted to safely and securely transfer information from one party to another. We apply the same rigor and care to handling both personal and non-personal data in the digital age. Today, consumers and businesses continue to rely on us to deliver their letters and parcels from Dublin to Nicosia, while protecting the mail's integrity and security.

PostEurop's members collect, process, transmit and store a large amount of data, including electronic data. This includes data on the sender, the receiver and the postal items themselves. We are driving through a range of product innovations and service improvements which are mostly driven by data. The future of Europe's logistics and delivery services will be driven by data, and we are using information to better respond to customer preferences, keep people informed of their deliveries and facilitate timely communications. We also hold data for other purposes such as customs clearance or security purposes, for operational efficiency (e.g. sorting, transportation and optimising delivery rounds), and direct marketing.

The European Commission's proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications ("the ePrivacy regulation", hereinafter "ePR") was written for the telecoms sector and "over the-top players" offering the same services as telecoms operators. However, it does not give proper consideration to the consequences that the new rules could have for other operators which may fall within the scope, albeit unintentionally. As a result, PostEurop's members would like to share their thoughts on the ePR under negotiation.

1. The link between GDPR and ePrivacy

The national posts have reliable processes and procedures in place to manage compliance with existing data protection legislation. With GDPR's entry into force on 25th May 2018, we have reviewed these processes and procedures to ensure they are fit for purpose. As such, PostEurop's members support wider industry calls for consistency and coherency between GDPR and ePR, particularly when it comes to asking for consent.

We believe GDPR's risk-based approach should also be present in ePR, as should GDPR's weighing of interest between the legitimate interests of providers and fundamental rights. Unlike GDPR, as

drafted ePR does not take into consideration the context in which the processing takes place, nor the impact on the individual's privacy.

GDPR recognises pseudonymisation as an appropriate safeguard when processing personal data whereas ePR only acknowledges anonymisation. PostEurop believes pseudonymisation should be viewed as an appropriate safeguard in ePR to be consistent with GDPR.

Furthermore, Chapter V of GDPR deals with the transfer of personal data to third countries while ePR deals with the transmission of electronic communications data. The relationship between the two is particularly important for postal operators which are increasingly exchanging/transmitting electronic personal and non-personal data linked to the movement of cross-border postal items to third countries. We cannot always ask for explicit consent from the receiver (in the third country) when the postal item and associated data enters our networks. As a result, PostEurop asks decision makers to ensure the procedures the posts are putting in place for electronic international data transfers under GDPR will not need to change under ePR.

Postal operators collect and process personal and non-personal data including metadata for various legitimate purposes. The transmission of such data to third parties is necessary for the provision of the postal services, for example for track and trace, customs clearance or security purposes. This transmission may be affected by ePR. As drafted, the storage or interception of such data during the transmission phase can only be done with the explicit consent of the data subject. We do not believe we are in scope. However, if we were considered within scope, this may place an unnecessary restriction on the operational flow and processes of postal operators. Also, it should be noted that in ePR, electronic communications include both content and metadata. This distinction does not apply to postal service providers' transmission of information related to the delivery of postal items.

2. Electronic communications services

PostEurop's members question whether some of their services could fall into the definition of an "electronic communications service" under the new regulation that refers to the definitions in the new European Electronic Communications Code (EECC). Again, we do not believe this is the intention of the legislators. However, the concrete application of this concept to postal processes and systems is unclear and leads to some confusion. Today, national postal operators exchange electronic data "wholly or mainly in the conveyance of signals" to provide postal services.

We are therefore concerned that ePR could capture some postal services, albeit unintentionally. For example, the International Post Corporation (IPC) handles the data transfers for the cross-border track and trace services the national posts offer. This sits on top of a traditional telecom provider. While in traditional terms, track and trace is not a public service (it is a service the sender buys), given that the service is available to everyone in Europe (anyone can go into a post office and buy an international track and trace product over the counter), we are concerned that we might fall within the scope.

3. Machine-to-machine (M2M) services

PostEurop's members also ask for further clarification when it comes to the definition of machine-to-machine (M2M) services under recital 12 of ePR.

The Council supports keeping the transmission services used for the provision of M2M services in the scope of ePR. It is also of the view that the distinction between the transmission and application layers and the relevant definitions was sufficiently addressed in the EECC. While the transmission layer constitutes an electronic communications service, the application layer is out of the scope.

National postal operators are increasingly deploying connected devices using electronic communications networks to provide their services. For example, delivery operators may convey signals over a network for track and trace purposes with a clearly defined purpose (providing a high-quality service to the sender and receiver of a parcel). This can be at various points in our network, as well as with the sender and the receiver.

We believe that applying ePR to postal processes and other IoT service layers would be inconsistent with the aim of ePR, which is to protect individuals' privacy rather than restricting universal service providers in the postal sector. It is also important to underline that ePR covers personal and non-personal data. Machines are increasingly communicating between themselves, and it does not necessarily include sensitive or personal data. It would be counterproductive to apply such restrictive rules to machines only exchanging technical information. Rules pertaining to M2M services should therefore be excluded from the regulation.

4. Direct marketing

The proposed article 8 of ePR aims to protect users' information stored in and related to end users' terminal equipment. This article remains technologically neutral but the main intent is to legislate the use of cookies and other technologies enabling online tracking. However, the collection of personal information from an end-user's terminal equipment is already submitted to the rules laid down by GDPR for the processing of personal data. GDPR has a flexible approach. It requires user consent, but also permits data processing in cases when it is needed for the performance of a contract, or when the service provider can show that either he or a third party have legitimate interests (as long as the rights of data subjects don't prevail). On the other hand, ePR limits the legal basis to user consent, without allowing for other legal grounds. In this respect, PostEurop considers that the ePR should include other legal grounds or further exceptions that allow for the data processing other than consent.

From a practical point of view, requiring systematic consent would impact users' online browsing habits with consent requests. Council discussions on some provisions are going in the right direction but need further work. For example, the text continues to suggest the deletion of article 10 on browser privacy settings. However, several Member States do not support its deletion and would prefer to reword it. PostEurop members consider that requiring browsers to prevent third

parties to access the device would provide them with disproportionate power within the online ecosystem. This solution goes against GDPR's approach because centralised consent through browsers would neither allow customers to give a specific nor an informed consent. The legislators should adopt rules allowing a dialogue with the user when consent is needed. Such a mechanism, based on the expression of the choice of the user, would provide more flexibility for actors to communicate with users and ask for consent but only when necessary.

In addition, article 16 provides a framework to determine the condition under which lawful direct marketing communication can take place. PostEurop is concerned by the lack of focus on this issue and calls on legislators to assess the scope and implications of article 16 and its related recitals.

Indeed, leaving the debate as it is could have a negative impact on direct marketing. The first problem we identified is the definition of direct marketing communications (art 4.3 (f). The European Parliament and the Council show that the legislators still need to work on this definition to avoid such harmful consequences for companies. It should be aligned with industry practice and defined by the two cumulative elements of being sent or directed (not presented) to particular individuals (not a broad group), thus excluding display advertising from the definition, regardless of the context in which display advertising takes place. Another problem raised during Council discussions is the ability for organisations to communicate with their existing clients (art. 16.2a). This possibility is essential because it allows brands to engage directly with their existing and prospective clients, enabling stable and interactive customer relationships leading to economic growth in Europe. Additionally, each product has a different purchase cycle and is linked to a different marketing strategy. Therefore, the Council's proposal to develop a national rule to impose a time limitation on the use of customer's contact details would fail to meet the objectives of the digital single market. Finally, postal operators call on legislators to clarify rules regarding B2B direct marketing communications. Those activities often benefit from a more flexible legal framework at the national level due to its business-only nature and the need for business to attract new clients and grow. Clarification is needed so that ePR does not require consent for B2B marketing sent to end users who are legal persons and individuals in their professional capacities.

Conclusions

As drafted, ePR is more than a "lex specialis" of GDPR. It introduces new and more stringent rules which could impact postal operators. For example, ePR restricts the processing of personal data to consent. This creates a "one size fits all" solution, which is unworkable for both businesses and their customers. We believe the text should be drafted to facilitate innovation and data flows in the postal sector. This would ensure we can continue to serve our customers, consumers and small businesses, across Europe.

ePR should be drafted to complement existing rules, minimise overlap and stay true to the objectives of data protection and telecoms law. For instance, anonymous data, which does not pose privacy risks and is therefore not covered by GDPR, should not be regulated. Rules pertaining to M2M platforms as well as data transfers between postal operators that are necessary to ensure we can continue to operate should be excluded from ePR and GDPR should apply.

Finally, sufficient time for implementation is needed as companies will need to apply software changes to comply with ePR and this requires at least 18 if not 24 months to implement.

For further information and action please contact:

Ms Elena Fernandez-Rodriguez
Chair of the European Union Affairs Committee at PostEurop
E: elena.fernandez@correos.com

Association of European Public Postal Operators AISBL

Association des Opérateurs Postaux Publics Européens AISBL

PostEurop is the association which represents the interest of 52 European public postal operators. Committed to supporting and developing a sustainable and competitive European postal communication market accessible to all customers and ensuring a modern and affordable universal service, PostEurop promotes cooperation and innovation bringing added value to the European postal industry. Its members represent 2.1 million employees across Europe and serve to 800 million customers daily through over 175,000 counters. PostEurop is also an officially recognised Restricted Union of the Universal Postal Union (UPU).