Telia

Offentlig

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

Innsendt elektronisk via departementenes hjemmesider

Dato
2017-03-20

Kontaktperson
Lars Vinden
45 88 85 54
Lars.vinden@telia.no

Referanse
17/482

Høring - EU-kommisjonens forslag til kommunikasjonsvernforordning – Saksnr 17/482

Telia Norge AS (Telia) viser til Samferdselsdepartementes høringsbrev 02. mars 2017 vedrørende EU-kommisjonens forslag til kommunikasjonsvernforordningen. Frist for innspill er satt til 20. mars 2017. Dette høringssvaret gjøres på vegne av hele Telias norske virksomhet, som omfatter merkevarene Telia, Chess, One Call og MyCall.

Telia eier og driver et landsdekkende mobilnett i Norge. Med en markedsandel på i overkant av 40 % er vi Norges nest største tilbyder av mobiltjenester. Som en del av Telia er vi også Nordens største mobiloperatør.

Vi vil i dette høringssvaret kommentere de mest sentrale endringene i lovforslaget, samt vedlagte uttalelse fra vårt morselskap Telia Company AB.

1 Generelt om behovet for ny regulering

Som en tilbyder av elektroniske kommunikasjonstjenester er Telia opptatt av at borgerne har et sterkt person- og kommunikasjonsvern. Vår generelle oppfatning er likevel at disse behovene i stor grad er hensyntatt gjennom EUs personvernforordningen (forordning 2016/679 – heretter GDPR), som innføres våren 2018 som en sektoruavhengig forordning som tar sikte på å styrke individenes personvern, samtidig som den skal tilrettelegge for innovasjon og fri flyt av personopplysninger over landegrensene. Etter vårt skjønn gir GDPR en hensiktsmessig og balansert tilnærming for å sikre enkeltindividenes personvern, samtidig som tjenestetilbyderne gis rimelige muligheter til å innovere og utvikle tjenester som er nyttige både for enkeltindivider og samfunnet.

Gitt veksten i kommunikasjon som foregår via såkalte OTT-tjenester, mener vi at det er avgjørende at en eventuell ny forordning er helt teknologinøytral. Vår oppfatning er at behovet for teknologinøytralitet best ivaretas gjennom sektoruavhengig regulering, da dette fullt ut tar høyde for teknologikonvergens og annen utvikling.

Med unntak for konfidensialitetskravet for elektronisk kommunikasjonsinnhold tilhørende juridiske personer, kan vi heller ikke se at kommunikasjonsvernforordningen gir vesentlig bedre vern for brukere av elektroniske kommunikasjonstjenester (og selv i disse tilfeller vil alt det vesentligste av kommunikasjonen være omfattet av kravene om konfidensialitet m.m. i GDPR).[1] Vi mener følgelig at det ikke er behov for en spesifikk regulering av personvernet knyttet til elektroniske kommunikasjonstjenester, og at forordningen således ikke bør innføres.

[1] Dette skyldes at de elektroniske kommunikasjonsdataene for juridiske enehter i de fleste tilfeller også vil kunne knyttes til identifiserbare enkeltpersoner (dvs ansatte hos den juridiske enheten, eller eventuelt kommunikasjonsmotparten)

Dersom en først skal innføre en sektor-spesifikk regulering, stiller Telia seg likevel positiv til at området reguleres som en forordning. Kommunikasjonstjenester er stadig mer internasjonale i sin natur, noe som særlig er synlig i de såkalte "Over-The-Top-tjenestene (OTT-tjenestene), og en forordning vil bidra positivt i forhold til konkurransesituasjonen mellom ulike aktører gjennom å sikre like spilleregler uavhengig av hvor tjenesten leveres fra. Ettersom Telia i Norge benytter en del systemer som leveres fra Telia Company sentralt, ser vi også operasjonelle fordeler i å ha en harmonisert tilnærming på tvers av landegrensene. Som følge av dette mener vi at også at eventuell adgang til særregulering i medlemslandene bør begrenses, eller eventuelt også harmoniseres på tvers av landegrensene.

2 Behandlingsgrunnlag og samtykke

Mens GDPR gir en rekke ulike og likeverdige grunnlag for å behandle personopplysninger, begrenser kommunikasjonsvernforordningen adgangen til å prosessere elektronisk kommunikasjonsdata (kommunikasjonsinnhold og metadata) til enkelte definerte behandlingsformål, med mindre brukeren har gitt sitt samtykke. Selv om vi er enige i utgangspunktet om at det må foreligge klare rammer for prosessering av elektronisk kommunikasjonsdata, mener vi at listen over lovlige behandlingsgrunnlag er for snever til å dekke rimelige behov hos tjenestetilbyderne, herunder behov for utviklingen av nettverkskvaliteten og andre aktiviteter som gir brukerne klare fordeler uten klart negative personvernkonsekvenser.

Som eksempler kan nevnes at tjenestetilbyderne må ha mulighet til å benytte allerede innsamlede metadata for å sikre hensiktsmessig kapasitet og kvalitet i nettverket, og det bør også være mulig å analysere forbruksmønsteret til en kunde for å gi anbefalinger om abonnementer som er bedre tilpasset den enkelte kundes bruksmønster. Begge disse eksemplene er behandlinger som etter vårt skjønn ville vært tillatt etter GDPR etter "legitim interesse"-kriteriet, og hvor personverninteressene til kundene ivaretas på en god måte i GDPR gjennom de generelle personvernprinsippene om dataminimalisering, sikkerhet osv, samt gjennom kundenes mulighet til å reservere seg mot behandlingen av data for de aktuelle formål. Vi viser i denne forbindelse til gjennomgangen av aktuelle behandlingsformål i uttalelsen fra Telia Company.

Vi er også skeptiske til kravet i artikkel 9.3. om å minne brukerne på adgangen til å trekke tilbake samtykker, og er enige i Telia Companys uttalelse om at denne typen krav kan bidra til at brukerne rett og slett går lei av informasjonen og samtykkene, slik vi i stor utstrekning har sett for cookie-reguleringen.

3 Personers rett til kontroll med elektroniske kommunikasjonstjenester

I likhet med Telia Company mener vi at bestemmelsene knyttet til nummervisning m.m. i artikkel 12-14 er i ferd med å bli utdaterte som følge av den tekniske utviklingen, og viser til vedlegget for en nærmere redegjørelse.

4 Tilsynskompetanse

I utkastet til forordning foreslås det at tilsynskompetansen for kommunikasjonsvernsforordningen skal være den samme som for GDPR, hvilket i Norges tilfelle vil si Datatilsynet. Selv om vi ser en del fordeler ved at tilsynskompetansen for personvernspørsmål samles hos ett organ, mener vi at overføringen av tilsynskompetanse kan medføre at tilsynsmyndighetene mister mye av den sektor-spesifikke fagkompetansen som NKOM besitter i dag knyttet til sikkerhet og beredskap m.m. Gitt at NKOM skal fortsette å ha tilsyn på disse områdene etter ekomloven vil NKOM og Datatilsynet fremdeles ha til dels

overlappende tilsynsområde. I en slik situasjon mener vi det er mest hensiktsmessig at NKOM fremdeles er tilsynsmyndighet for reguleringen av elektroniske kommunikasjonstjenester.

Selv om det ikke omtales direkte i høringsbrevet, antar vi at utkastet til forordning også medfører at tilsynskompetansen for uanmodet elektronisk markedsføring, som i dag er regulert i markedsføringsloven § 15, overføres fra Forbrukerombudet til Datatilsynet. Av erfaring vet vi at saker etter markedsføringsloven § 15 ofte innebærer brudd på andre bestemmelser i markedsføringsloven, slik som villedende markedsføring og annen urimelig handelspraksis, og vi mener det vil være uheldig for forbrukervernet om tilsynskompetansen for denne typen saker skal bli spredt mellom to ulike tilsynsorgan. Vi mener derfor at Forbrukerombudet bør fortsette å føre tilsyn med bestemmelsen om uanmodet elektronisk markedsføring.

***

Dersom dere har ytterligere spørsmål i anledning saken kan dere ta kontakt med undertegnede.

Med vennlig hilsen
Telia Norge AS

Lars Vinden
Juridisk rådgiver/personvernombud

Vedlegg: Telia Company's opinion regarding the draft E-Privacy Regulation (EPR)

Telia Company

Telia Company's opinion regarding the draft E-Privacy Regulation (EPR)

Executive summary

- The proposed EPR brings no additional protection of personal data for electronic communications, which is not already ensured in the GDPR.
- Apart from the right to confidentiality, there is no evidence that processing of non-personal communication data needs special protection.
- There is a continuous gap between the draft EPR and GDPR, where there are both overlaps and gaps relating to how to apply GDPR to personal data that is processed based on EPR.
- The draft EPR Imposes unnecessary limitations on certain service providers, impeding the development of future services and products to the detriment of consumers and the future growth in Europe in key technology and communication sectors.

Data protection is one of the highest prioritized regulatory matters within Telia Company, it is therefore natural that the draft e-Privacy Regulation[1] (EPR) is also a focus area. As a telecom operator, most processing of personal data is data that is defined as meta or content data under EPR. The draft regulation implies that we will have to fulfill both the provisions under the EPR but also under the General Data Protection Regulation (GDPR)[2], when complimentary obligations are outlined in GDPR. One of the important goals of the GDPR is the fulfilment of fully harmonising the protection of personal data - across sectors and across EU/EEA. Additionally, when reviewing the old Data protection Directive[3], legislators at an early stage recognized the digital evolution and aimed at modernizing the Directive to the digital era. As an example, within the definition of personal data in GDPR[4] location data is now specifically outlined. GDPR will strengthen the individuals' rights when their personal data is processed, regardless if processing is taking place in relationship to a bank, insurance, medical or telecommunication services. GDPR represents a balance of protection of all types of personal data while ensuring that Europeans are continuously able to benefit from new services simplifying everyday life, and enabling service providers to develop services advancing our societies based on harmonized European legislation.

Telia Company is of the opinion that the current sector specific privacy legislation is outdated. Telia Company has been consistently pleading for a repeal of the e-Privacy framework. This since firstly the digital world has become increasingly convergent and secondly since we are of the view that the GDPR provides needed safeguards regarding information, transparency, right to object and the possibility to withdraw consent at any time as well as heavy sanctions for infringing companies.

[1] Directive 2002/58/EC
[2] EU/2016/579
[3] Directive 95/46/EC
[4] Article 4.1 GDPR

Company information
TeliaSonera AB
Stureplan 8 SE-10663 Stockholm, Sweden
Registered office: Stockholm
Business ID 556103-4249 VAT No. SE556103424901

The notion of a continuation of a sector specific privacy law in EU implies that the lawmakers do not acknowledging that the GDPR will fulfil its objectives, i.e. achieving a technologically neutral, future-proof and flexible framework while ensuring Europe's high standards in the protection of personal data. We very much disagree with the proposal that GDPR should be seen as inadequate; we believe that the GDPR will immensely strengthen individuals' rights also in the communication sector.

We are of the opinion that the notation outlined in the Inception Impact Assessment[5] should be taken into account, namely where the Commission explicitly mentions the need to consider all policy options concerning simplification of the legal framework and consistency with especially GDPR where outdated and unnecessary provisions in the e-Privacy Directive should be repealed. Already in 2015, an independent study carried out for the European Commission on the e-Privacy Directive (assessment of transposition, effectiveness and compatibility with GDPR)[6] concluded that maintaining a distinct regulatory regime for electronic communications services, information society services or audiovisual services would most probably become less and less relevant in the future.

In our mind, it was a mistake by that the Commission to remain the full scope of the EPR and hence provide for a double set of rules based on an old structure of thinking. The two set of rules will continue to cause confusion for businesses and consumers, and will hamper the possibility of communication providers to develop innovative services, especially in the area of big data which is seen as key in developing future digital societies. Please find below examples supporting our view as well as opinions of other provisions.

1 Regulation compared to Directive

If a sector specific privacy law is deemed necessary, we support that the legal instrument is a Regulation rather than a Directive. The reason is that the e-Privacy law is *lex specialis* to GDPR, and GDPR will be applicable to all matters not specifically addressed by the EPR. A regulation is therefore necessary to ensure consistency between the two instruments. For a company such as Telia Company that has a lot of centralized systems, it is necessary to have fully harmonized requirements in our European footprint. Currently, we have several issues due to the fact that the e-Privacy Directive has been implemented in such a divergent manner across our operations.

We are also worried about the exception provided in article 11 EPR, concerning Member States possibility to restrict article 5-8 of EPR. In order to provide equal level of protection, to ensure a free flow of communication data across Europe, as well as lower compliance costs for business there should be a very limited exception to the stipulated rules. Recital 26 outlines in more details when a Member States could possible restrict the law further, however, since the law has fully taken into account the ECHR obligations, such restriction should not be necessary.

2 Material Scope

Currently, the e-Privacy Directive provides for a different scope than the GDPR; outlining protection of data that is non-personal communication data and data related to legal person, in addition to personal data that

[5] Inception Impact Assessment – REFIT Evaluation and Impact Assessment of Directive 2002/58/EC (October 2016)
[6] SMART 2013/0071, June 2015

would be covered by GDPR. Telia Company believes there is little evidence to support the notion that there is a need to provide for additional protection of non-personal data and protection of data related to legal people.

In reality, when communication data is being processed under the subscription of a legal person, the vast majority of the data will be sufficiently associated with the individuals using the communication service (e.g. employees or customers of the legal person), to constitute personal data under the GDPR. As such, we believe for the most part that the overlapping provisions in EPR are unnecessary.[7]

We continuously question the need for a special privacy Regulation for communication services, however if legislators finally agree to adopt the EPR, then as many provisions as possible should better correlate and complement the GDPR. The material scope outlined in Article 2 EPR and the definitions in article 4.1 and 4.2 EPR has created numerous uncertainties already. The definition outlined in Article 4.2 means, as we interpret it, that the scope of EPR is extremely wide (e.g. a large number of companies would have customer service chat functions where EPR would apply). We consider the scope artificial, and with unclear boundaries. To give an example of this, many companies are processing IP addresses to provide internet based services. A majority of these companies would not fall within the definitions outlined in Article 4 EPR. i.e. not defined as communication providers why the EPR does not apply to them. Nonetheless, this processing of IP addresses would often be considered as processing of personal data, why GDPR will apply. In our mind this means that the same data is being processed for delivering different types of services but different laws applies due to the scope of EPR.

3 Legal grounds under EPR

The Commission has in their REFIT evaluation concluded that the so called Cookie provision (Article 5(3)) e-privacy Directive, was unfit for its purpose and has therefore revised it to allow usage of cookies without prior consent, when they are seen as non-privacy intrusive. As a reason for altering this provision, the Commission states that it was over-inclusive. Telia Company is of the opinion that the same method of evaluation should have been used for all metadata and content data processing. Processing of metadata, like processing of other personal data, can be carried out in a manner that is non-privacy intrusive. Additionally the concept that consent is seen to always provide the highest level of protection should in our mind be questioned. Here there are direct learnings to be drawn from the *privacy fatigue* the current cookie provision has led to, without providing for strengthened protection of data subjects' privacy.

Under GDPR data controllers have the burden of proving that they are only processing personal data for a specified, explicit and legitimate purpose and with an applicable legal ground. GDPR was meant to cut red-tape and strengthen the internal market by focusing on data controllers accountability and ensuring compliance by applying strict sanctions. EPR does not acknowledge the focus on accountability and once more, in a very detailed manner, describes how to process communication data. Telia Company is of opinion that this represents an over-regulation that will only hamper innovation, and potentially limit services that would also be of great benefit for users and society as a whole.

---

[7] See section 3 for a discussion of whether additional provisions to safeguard content of communications associated with legal persons should be offered.

Besides consent, GDPR recognizes other legal grounds for processing personal data like legitimate interest or performance of a contract. For processing of personal data to be lawful under GDPR the data controller must, in addition to demonstrating a legal ground, fulfill the Chapter III rights in GDPR, which provides for various strict obligations to secure data subjects' privacy is protected sufficiently. Based on the GDPR, the data controller is asked to strike a balance between its legitimate interest and the fundamental rights and Freedoms of the data subject. This differs between GDPR and the draft EPR: the former allows/obliges the controller to do a thorough assessment weighing its interests with the interests and fundamental rights of the data subject and it will not be able to process if its interest is overridden by those of the data subject data. Based on above we believe that article 6 EPR should be fully aligned with article 6 GDPR. It goes without saying that in case of electronic communications data, the balance of interests may lead to a different conclusion of appropriateness than for other types of personal data.

Article 6 of the EPR outlines that for processing of e-communications data ("content" and "metadata") the general rule is consent, which builds on the wrongful notion that there is a hierarchy between the different legal grounds.[8]

Only for the following types of processing is consent not needed:

- for the transmission of the communication and detecting faults and errors when carrying out transmission
- to maintain or restore security
- to meet mandatory quality of service requirements pursuant to the Code and the Net Neutrality Regulation
- for billing, payment and interconnection
- fraud and abusive usage of the service.

Without prejudice to the above points, metadata will need to be erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication.

Telia Company supports rules that ensures that processing of content and metadata is done on the data subjects' terms, which prevents abusive behaviors, by controllers. However, we think that the proposed rules in Article 6 are disproportionate and stand in the way of a range of legitimate data processing purposes:

- Network development and fault handling: The use of electronic communications data for the management and improvement/roll-out and commercially driven quality improvement of the electronic communications networks is not explicitly foreseen by Article 6. Network engineers

[8] See WP29/2017. For example, consent is just one of several legal grounds to process personal data, rather than the main ground. When correctly used, consent is a tool giving the data subject control over the processing of his or her data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

need to monitor metadata (e.g. measure the usage or throughput per mobile cell, or the usage habits in a certain fixed network area) and to certain extent even content data (e.g. measure which applications impact throughput) in order to be able to efficiently manage traffic, and to take rational decisions as regards network investment and roll-out planning (where to install more mobile antennas, when/where to acquire network nodes etc.). Anonymised meta- and content data will not provide the necessary information needed to carry out essential network monitoring or planning.

Under GDPR the above outlined purposes would normally be lawful because of the legitimate interest of the controller overriding the interest of the data subject. Network coverage, quality and capacity are fundamental attributes to providing customers with communication services, and we believe that a limited processing of identifiable data is necessary to provide state-of-the-art services to customers. Our customers are continuously asking for, and expecting, improvements in quality to such an extent that it should be considered that the data subjects reasonably expect telecom operators to carry out limited processing for this specific and explicit purpose. However, under EPR telecom operators will not be legally allowed to efficiently improve the quality of their services and their networks, unless data subjects provide their consents. Obtaining consents for this type of processing that is limited in scope, with a rational, specific and explicit purpose, and for data that is already processed for other legitimate purposes, may in our view cause additional "privacy fatigue". On a more fundamental note, one could also argue that processing of communication data to improve the communication networks is beneficial for every user of the network, and not only to those that consent to such processing. As such, it is somewhat unreasonable to allow certain individuals to be free-riders to a processing activity that is fundamental to operating networks, and as such providing high quality services to the same individuals.

- Product development: Article 6 does not explicitly allow the use of electronic communications data for the development of products and services.

  In order to efficiently develop products and services that correspond to the needs of our customers, telecom operators use aggregated information, which in an initial phase is based on e.g. on usage of non-anonymized metadata (% of roaming, divided over various locations, % of calls to fixed/mobile numbers, development of mobile data usage, etc.). As outlined above, it can be argued that processing for this specific purpose is something the data subject would reasonably expect. Customers who do not want to be subject to such processing may object under GDPR Article 21. This mechanism offers a reasonable balance between the interest of the service provider and society at large on one hand and the individual rights and freedoms on the other, and is clearly favourable to the EPR's inefficient and disproportionate prohibition of such use of metadata.

- Customer benefits: Article 6 does not allow the use of metadata for direct marketing or customer care purposes.

  Does that mean that telecom operators could not propose a more adapted tariff plan to a customer whose metadata shows that his/her tariff plan is not well adapted to his/her effective

service usage, e.g. when he/she uses a small amount of the calls but always exceed the data bucket, without asking for a consent for this explicit and specific purpose? Neither can a telecom operator process personal data to improve customer care making sure the most efficient services to their customers.

- Purpose: Of extra concern is the fact that Article 6 outlines that even with consent metadata and content data may only be processed if the explicit purpose could not be fulfilled with anonymised data. Under Article 5 GDPR, the rule of *data minimisation* is outlined which stipulates that data shall be adequate, relevant and limited to what is necessary in relations to the purpose. It seems that EPR goes beyond this rule and again provides additional detailed obligations, without outlining the need for it.

  Additionally, the fact that prior consent is needed for all situations not explicitly stated in Article 6 make it very difficult for telecom operators to make interesting and society-valuable location analyses that concern somewhat longer periods, benefiting for example sectors as tourism, mobility, etc. It would therefore benefit from the more balanced GDPR regime, which explicitly recognizes the possibilities of legitimate interest and compatible purposes, of course attached with strict information obligations and security measures such as pseudonymisation. We do not see that this difference in treatment is justified. Here it should be noted that under GDPR processing of location data is not seen as processing of a special category of data as outlined in Article 9 GDPR. Therefore, it is surprising that the processing of location data, when carried out by a communication provider, obliges consent.

In addition, we believe that processing for a secondary purpose compatible with the original purpose, as outlined in Article 6.4 GDPR, should be permitted also under EPR.

If legislators decide to maintain EPR in addition to the GDPR, the proposed Article 6 EPR should be modified in order to align with Article 6 GDPR incorporating the additional legal grounds.

4 Confidentiality of communication

As described by the European Commission in the explanatory memorandum, there is a need to ensure an effective legal instrument that protects Article 7 of the Charter, where the scope is also communication of legal persons. Since this is not covered by GDPR, it should be covered elsewhere.

5 Storage and erasure of electronic communication data

Electronic communication data, like personal data under GDPR[9], should only be processed as long as it is necessary and kept up-to date for its purpose. What is outlined in Article 7 EPR does not bring any additional rights or benefits to what is outlined in GDPR and has in our view no additional purpose. Therefore, Telia Company believes that it should be repealed.

[9] As outlined in article 5.1

6 Consent

The conditions of consent has been strengthened under GDPR, by for example outlining that a consent would not be seen as freely given if the performance of a contract is conditional on consent. In the draft EPR, article 9.3 proposes an additional condition compared to GDPR, namely that the communication provider shall remind the *end-user* every six months of the possibility to withdraw their consent, which is unnecessarily burdensome on communications providers as well as end-users.

Processing of personal data and communication data is done in a majority of cases for the benefit of the data subject (e.g providing the service) and/or society as a whole (e.g. improving network quality or big data analytics). GDPR has established both a balance for ensuring a high level of data protection (based on strict legal grounds and rights of data subjects stipulated in chapter III) while also ensuring that the digital economy can blossom, innovate new services and assist society. Under EPR, the lack of all legal grounds will in our mind create a *privacy fatigue,* which means data subjects will likely be overwhelmed by consent requests as was the situation with the Cookie provision under e-Privacy directive.[10] If, in addition to these consent requests, data controllers must remind data subjects every six months, we are worried the whole notion of consent will be utterly weakened and therefore not provide additional privacy and data protection.

Data that is being processed based on a valid consent under EPR may often, as outlined under section 2, be personal data where the data subject has individual rights under GDPR. If a legal person is the end-user and has given consent, as outlined in Article 6 and 9 EPR, how should a commination provider handle for example a data subjects right to object (as an example) to having his/her personal data processed? In our view the solution should be to only remain the rules under GDPR.

7 Rights to control electronic communications and unsolicited communications

Currently a lot of detailed rules exist in the e-Privacy Directive concerning call records, automatic calls forwarding, directories etc. Some of these have been removed, however number presentation remains and new very detailed provisions have been proposed. Telia Company wonder how wide spread the problem the Commission is trying to solve with these provisions are. For example in Telia Company's footprint the number of households and businesses with fixed telephony is declining every year, at the same time smart phone penetration is increasing rapidly. On most feature and smartphones, it is possible for the user to both identify the number calling and hide their own number when making a call, therefore we are of the opinion that Article 12 and 13 are superfluous. The same reasoning goes for incoming call blocking where it is very easy to "blacklist" numbers on your smartphone. Since these solutions already exist for a great majority of users within our footprint the proposal seems not be the least intrusive measure to reach a solution. We therefore propose to abolish also article 14.

The draft EPR outlines that direct marketing calls shall have its own prefix or provide identifiable numbers. Firstly, article 16 *Unsolicited Communications* applies to all undertakings providing direct marketing calls, email, sms etc, and not just communication providers, and would therefore be better placed in a generic regulation. Secondly, the existing rules on unsolicited communications have in our mind fulfilled its purpose why the concept of pre-fix seems to try to solve a non-existing matter and would therefore be redundant. Thirdly, we are yet again wondering if there are less intrusive measures that can

[10] As is described in recital 22 EPR

be applied to overcome this claimed problem; smartphones are providing the possibility to black list calls from individual numbers, such as direct marketing companies.

To monitor and implement solutions for article 12-14 and 16.3 is costly for telecom operators and if there are already available solutions it should be scrutinized if these provisions firstly, are needed to solve a real problem, secondly, if the solution proposed is the least intrusive and most cost efficient.

8 Security risks

Concerning the security rules, we wonder if there is a real need to have specific security rules in EPR, next to those outlined in GDPR. In the draft EPR, Article 17 proposes that electronic communication providers should inform the subscribers if there is a particular risk of a breach.[11] In some cases however, a notification will compromise the security of the networks and the services even further. This has been recognized in the Finnish regulation, which stated that: "*Before informing users, it is advisable to attempt to correct the security hole or other vulnerability in order to avoid additional damage to subscribers.*"[12] We propose to firstly rely fully on the GDPR rules but if the rule is kept, it should be altered so that Article 17 is in line with the current Finnish law in order to avoid an increased risk of network attacks.

9 Entry into force

There are several new provisions in EPR which will require IT alterations and developments (depending on the final outcome of the review). During the GDPR implementation project, we have learnt that all IT solutions take a vast amount of time to solve and apply. Therefore, as an absolute minimum communication providers must have 24 months implementation period after the EPR is adopted.

[11] Article 4.2 E-privacy regulation
[12] Finland Ficora has given Regulation no 66, section 10.2