Brief Study of Security and Spam Measures – Providers

Provider name	Telco □	ISP □	Content Provider □
Contact name	Phone	Email	Remain anonymous □

#	Question	Legal Reference
1.	In the context of information security and spam, what national legislation are you required to comply with?	
2.	Which of the following measures do you take in order to improve security of your services? Technical measures □ Ingress filtering □ Egress filtering □ Content filtering □ Quarantining an infected / malicious PC □ Blackholing/Sinkholing □ Secure Domain Name Service □ Traffic Shaping / Throttling Organizational matters □ Detailed written guidance for staff, partners and customers □ Free or subsidized security software for users □ Hotline/Helpdesk □ Clear contact details for email abuse and security violations □ Remote technical assistance (i.e. with access to the device) □ Regularly information to users (web, mail, email) □ Other (pls. specify):	Article 4 (Security), §1 The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, …
3.	Regarding these measures, do you work in conjunction with a public communications network provider? □ yes, we do □ no, we do not □ we are also a public communication network provider ourselves	(cont.) … if necessary in conjunction with the provider of the public communications network with respect to network security.
4.	How do you take into account state of the art and cost of the implementation to ensure an appropriate level of security? Please prioritize the following options (1,2,3): We follow guidance in international standards We follow guidance in national legislation & annexes We follow the advice of our national computer security organization We follow industry best practice We do what is necessary based on our own risk assessments We do not necessarily feel that guidance or any measures are needed	(cont.) Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
5.	How do you become aware of security or spam problems? □ We rely on the complaints of our customers □ We monitor for traffic peaks □ We have deployed real-time traffic anomaly detection Others (pls. specify)	*(cont.)*
6.	If you become aware of a particular risk of a breach of the security of your network, what do you do? □ We inform subscribers directly (e.g. via email) □ We inform our customers via open channels (e.g. via a press release or a note on the website) □ We report to our National Regulator □We regularly issue reports available to the public (e.g. every 3-12 months) □ We decide on appropriate measures on a case-by-case basis □ There is no such provision in our national law, therefore, we issue no reports	Article 4 (Security), §2 In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk …
7.	If the risk lies outside the scope of the measures that you as a provider can take, what do you do? □ We inform our subscribers of any possible remedies that they can take □ We also inform them of the associated costs of such remedies □ We also inform them on the risk of not implementing counter measures □ We mandate measures and we are prepared to discontinue servicing non-compliant customers	(cont.) and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

8.	What measures did you put in place to prevent your customers from **sending** unsolicited communications (spam)? □ We inform them about the legal consequences □ We forbid it in our Terms & Conditions □ We blacklist (MAPS, Spamhouse, NJABL) them if they repeatedly send spam □ We greylist them if they send spam until they stop it □ We whitelist all our customers who do not send spam □ We reject all straight SMTP traffic from consumer connections □ We do not interfere in the content of our customers communications □ We do nothing but we wish we could do more □ We admit that some of our customers are spammers What measures did you put in place to protect your customers from **receiving** unsolicited communications (spam)? □ We offer spam-filtering on our network free-of-charge □ We offer spam-filtering on our network for an additional fee □ We offer software free-of-charge that customers can install on their computers □ We offer commercial software that customers can install on their computers □ We do not interfere in the content of our customers communications □ We do nothing but we wish we could do more	Article 13 **Unsolicited communications** 1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
9.	Does legislation in your country allow unsolicited communications for purposes of direct marketing only with the consent of the subscriber (opt-in)? □ yes □ no Does legislation in your country allow unsolicited communications for purposes of direct marketing unless the subscriber expressed the wish to no receive these communications (opt-out)? □ yes □ no	3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.
10.	How do you prevent senders of electronic mail from disguising or concealing their identity? We implement the following sender authentication mechanisms □ SMTP Authentication □ Sender ID Framework (SIDF) □ Yahoo's Domain Keys (DKIM) □ Cisco's Identified Internet Mail Other (pls. specify)	4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.
11.	What sort of measures do you take if you detect spam coming from an ISP based in a non-EU country □ We contact that ISP to discuss countermeasures □ We address the problem of spam in inter-connection agreements □ We filter or block SMTP traffic from that ISP if the ISP itself does not take measures against spam □ We inform our National Regulatory Authority □ We pursue legal actions □ We do nothing but we wish we could do more Other (pls. specify)	*(cont.)*
12.	If one or several questions above did not offer appropriate answer options, please use this space to explain. Please also indicate the number of the question.	