To whom it may concern,

I have some remarks to Guidelines 07/2020 on the concepts of controller and processor in the GDPR version 1.0.

In point 111. there is obligation for specifying type of personal data in the most detailed manner as possible, not only for special categories of data or relating to criminal conviction and offences. In some cases, it is only unnecessary formalism, which in occurrence of a cyberattack create dangerous recommendation where to look for particular interesting information for a (in many instances internal) hacker.

Those types of detailed information should be available only in case if it can improve safety or in other way amend processing of personal data, not just for convenience of supervisory authority.

For example, in service like hosting or similar activity processor should know there are special types of data which need higher safety conditions. – Additional information specifying which kind of sensitive data will be process should be omitted if it will not detriment the processing.

If there is a need for more specified terms and conditions to process for example data concerning health than sexual orientation, EDPB should in advance, maybe in guidelines, outline scale for special category of data which require more attention than the other.

In my opinion point 111. in that form is contrary to risk base approach introduced in DGPR, and to safety rule to not disclose information which is not necessary.

In point 133. recommendation to specify numbers of “e.g. numbers of hours” is counterproductive. Very useful in court but this stipulation creates psychological condition that processor thinks he has X hours to notify controller. In fact, there is no time to waste – it must be crystal clear to processor – without undue delay after discovery of data breach notify controller. If it is possible Immediately, without waiting one second. Every delay, conscious or not, may harm data subjects.

If X in the example is equal to 24 h according to art. 28(4) GDPR the same data protection obligations are set out to sub-processor. After three contracts with sub-processors there is no time for controller to notify supervisory authority (72h) if it is necessary.

I think in reality this addendum made position of data subject weaker rather than stronger.

Best regards,

Robert Żurakowski

Data Protection Officer

Email: inspektorochronydanych@mikrobit.pl

Mobile: +48 603 202 607