Non-paper by The Netherlands, Denmark, Belgium, Austria, Italy and Finland on a support period covering the entire expected product lifetime in the Cyber Resilience Act

One of the main objectives of the CRA is to not only ensure that products with digital elements meet essential cybersecurity requirements when they are placed on the internal market, but also to ensure that manufacturers have a duty of care throughout the product's life cycle. In the Commission proposal, however, the period in which manufacturers are obliged to provide effective vulnerability handling in accordance with the essential requirements ('support period') would not cover the entire duration of the product's expected lifetime. The proposal would therefore be insufficient in minimising undesirable situations in which users will continue to use a product that is no longer supported and therefore possibly not secure. Or, force users to discard products that otherwise still function, which is very undesirable from a sustainability viewpoint. To sufficiently contribute to safer ICT supply chains, the manufacturer ought to be responsible for effective vulnerability handling for the entire duration of the expected product lifetime.

This non-paper calls for:

1. the support period to cover the entire expected product lifetime - without maximisation;
2. the expected product lifetime to be determined by taking into account the time users can reasonably expect to use the product;
3. a requirement to clearly inform the user about the guaranteed cybersecurity support period and the year and month by which it ends;
4. market surveillance authorities to publish statistics on the expected product lifetime as determined by manufacturers.

1. Support period to cover the entire expected product lifetime

We oppose the use of a maximisation of the period during which the manufacturer is to ensure that vulnerabilities are handled effectively and in accordance with the essential requirements ('support period'), such as the 5 year maximum in the Commission proposal. Many products should be relied on for much longer than five years. Industrial control systems for example, should be relied on for at least ten or twenty years. The five year maximum in the Commission proposal could create a negative incentive for producers to only provide cybersecurity support for five years. Many users nevertheless will keep using a digital product that is no longer (guaranteed) cybersecure: either because they are not aware that their product is no longer cybersecure or because they are not able to replace the product (dependency).

We propose that the main rule in Article 10 (6) should be **that the support period covers the expected product lifetime**:

*"Manufacturers shall ensure, when placing a product with digital elements on the market **and for the expected product lifetime**, that vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I."*

Alternative wordings such as 'a support period *appropriate to* the expected lifetime' would seem to leave too much room for a manufacturer, for economic reasons, to choose a support period that is notably shorter than the period in which many users will continue to use the (then possibly not secure) product.

2. Reasonable expectations of users

The support period should be based on **the time users reasonably expect to be able to use the product** given its functionality and intended purpose.

In order to avoid a race to the bottom which would undermine its effectiveness, Article 10 (6) should also prescribe how the manufacturer is to determine the expected product lifetime referred to in the first subparagraph. We recognise that a manufacturer cannot be expected to provide updates for an unreasonably long period, for instance when a product in reality is used much longer than could have been expected at the moment of placing it on the market.

Similar wording is used in the digital content and digital services directives[1], according to which a consumer should be supplied with security updates for the period of time "that the consumer may reasonably expect given the type and purpose of the goods and the digital elements, and taking into account the circumstances and nature of the contract". For the CRA, which is not limited to consumer products, we propose to introduce the following subparagraph in Article 10 (6):

> *"Manufacturers shall determine the **expected product lifetime** referred to in the first subparagraph of this paragraph taking into account the time users reasonably expect to be able to **use the product given its functionality and intended purpose and therefore can expect to** receive security updates (…)."*

Implementing acts based on the Ecodesign directive[2] - where available - would indicate the absolute minimum expected lifetime for respective categories of products.

By setting as a main rule that the support period should cover the expected product lifetime, in combination with the transparency about the duration of this expected product lifetime (and therefore support period) proposed below, we expect most manufacturers to choose a reasonable support period[3]. Individual manufacturers could even try to stand out by committing to a longer expected product lifetime (and support period) than their competitors. If, however, a market surveillance authority receives indications that a manufacturer has opted for a period that is too short given the product's functionality and intended purpose, the national market surveillance authority could enforce compliance. The dedicated administrative cooperation group (ADCO) with representatives of national market surveillance authorities could serve to secure a uniform application of the obligation in Article 10 (6).

3. Clearly inform users about the actual support period

Users should be clearly informed about the expected product lifetime during which the manufacturer commits to provide security updates or otherwise effectively handle vulnerabilities. When comparing products, a possible end user should be able to take into account the actual support period to make an informed decision. This will contribute to manufacturers using a reasonable and realistic period of time, and could even serve as an incentive to stand out by committing to a longer support period than the competition.

The concrete date until which the manufacturer guarantees as a minimum to provide security updates should be clearly indicated on the product or its packaging, where applicable, and in another easily findable location (for example online). This information should at least be clear to the user at the moment of sale, but should also be available online during the support period. The guaranteed **minimum end date (month and year) should be indicated** rather than a number of years or months after which the product is placed on the market, which few users will know or desire to calculate. Such a clearly indicated end date also addresses the risk of distributors selling products

[1] Directive (EU) 2019/770 and Directive (EU) 2019/771.
[2] Directive 2009/125/EC.
[3] In the case of complex products used in industry settings with an expected lifetime of more than 10 years, consideration should be given to the possibility for manufacturers to charge a reasonable fee for the delivery of security updates after 10 years, but before the end of the expected lifetime, e.g. according to clear contractual terms agreed with the (non-consumer) user. This would be in line with current practice in some business-to-business (B2B) contracts, especially when products are sold to a limited number of clients and may entail some customised features

long after their placing on the market, leaving a shorter support period than these buyers in particular would otherwise expect.

To this end we propose the following wording for Article 10 (10a):

> *"Manufacturers shall **clearly and understandably specify** in an easily accessible manner and where applicable on the packaging of the product with digital elements, the end date for the expected product lifetime as referred to in paragraph 6, including **at least the month and year**, until which the manufacturer will at least ensure the effective handling of vulnerabilities in accordance with the essential requirements set out in Section 2 of Annex I."*

4. Market surveillance authorities to publish statistics on expected product lifetimes provided by manufacturers

Additional mechanisms to prevent manufacturers from applying an expected product lifetime that is too short could be considered. Market surveillance authorities should be allowed to publish statistics about the expected lifetime manufacturers have determined for their product, based on the indication of this expected product lifetime pursuant to Article 10 (10a). This would allow users to compare the expected product lifetime indicated on a product with digital elements they are considering to purchase with the average expected product lifetime provided for that category of products, and would serve as an extra incentive for manufacturers not to underestimate the expected product lifetime.

To clearly allow market surveillance authorities to publish statistics, we propose to add the following paragraph to Article 41:

> *"8a. Market surveillance authorities may publish statistics about the average expected product lifetime, as specified by the manufacturer pursuant to article 10 (10a), per category of products with digital elements."*