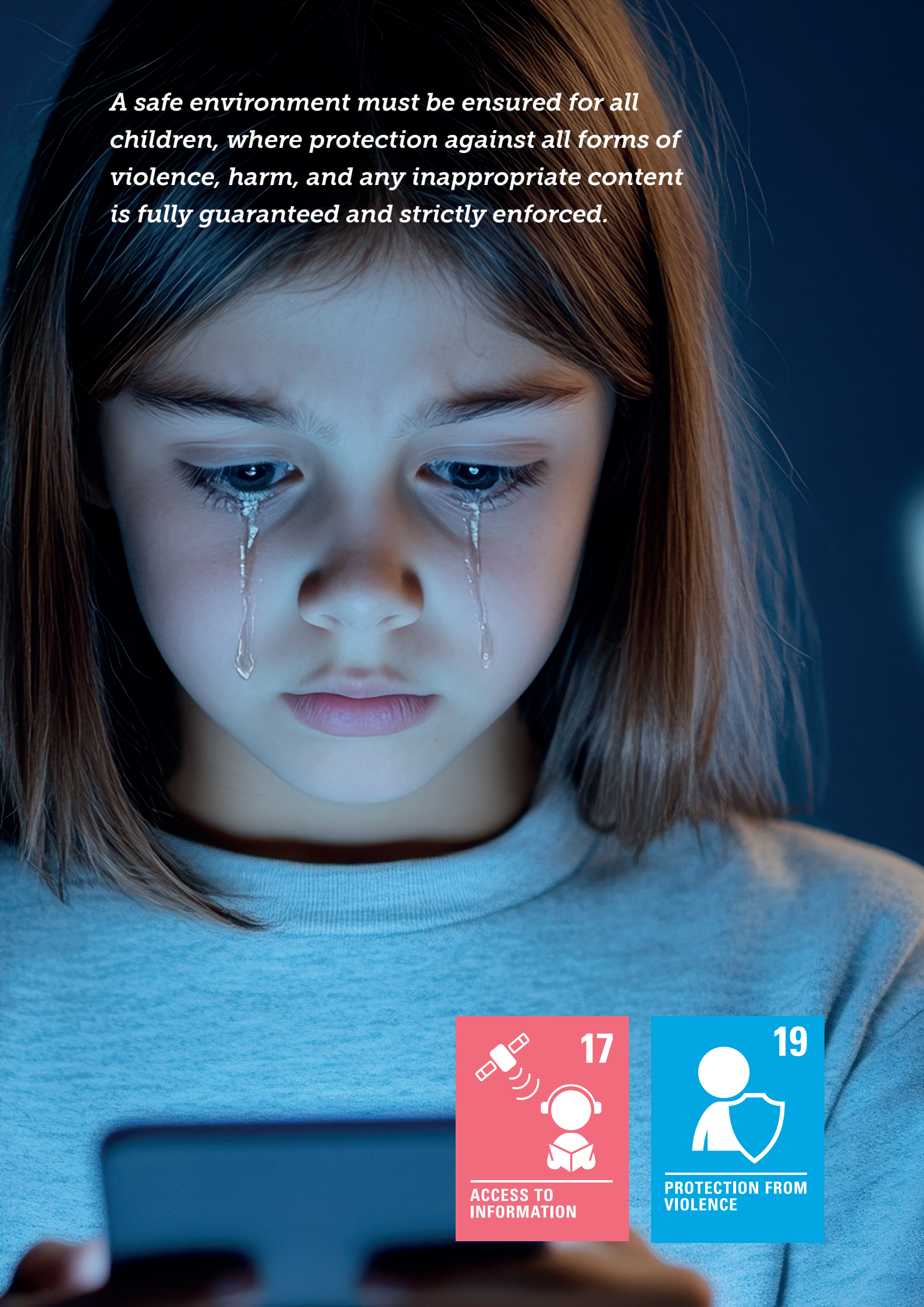
HANDOUT

Child protection in the digital world

Based on its 2024 and 2025 annual reports, the Ombudsman for Children and Adolescents (OKAJU) proposes comprehensive, child-centred recommendations to strengthen protection online, regulate access, prevent online violence, and ensure coordinated prevention, enforcement, and victim support.

Ombudsman okaju
fir Kanner a Jugendlecher


A safe environment must be ensured for all children, where protection against all forms of violence, harm, and any inappropriate content is fully guaranteed and strictly enforced.
17
ACCESS TO INFORMATION
19
PROTECTION FROM VIOLENCE

Recommendations from the
OKAJU's 2025 annual report regarding

Child protection in the digital world

1. **Place the best interests of the child at the core of digital policies**: the digital world must be designed and regulated in accordance with the requirements of the United Nations Convention on the Rights of the Child (UNCRC) (protection from all forms of violence, precautionary principle).
2. **Introduce a legal minimum age of 15 for owning any smartphone or device that gives unsupervised access to the Internet and social media.** Before that age, effective supervision and parental controls should be mandatory.
3. **Promote the development and availability of safe, child appropriate technological alternatives, such as restricted phones ("safephones") designed according to the "safety by design" principle**, for example allowing only communication and basic functions (no web browsing, no access to social networks or to unsecured networks).
4. **Require all platforms and digital services to implement robust, privacy preserving and interoperable age verification systems.**
5. **Ensure the systematic blocking of children's access to sensitive and harmful content,** including content – real, virtual or generated by artificial intelligence – that is pornographic or incest themed, promotes violence, involves child sexual abuse material (CSAM), or depicts adults presented as children. Explicitly prohibit the production, dissemination and promotion of such content on all platforms and put in place technical tools for its detection and immediate removal under the supervision of competent authorities. Provide for strong and proportionate sanctions in the event of non compliance, in line with European and international standards (DSA, GDPR).

6. Strengthen institutional and intersectional coordination:

   (a) Strengthen coordination between schools, families, associations, professionals, child protection authorities and cybersecurity actors.
   (b) Create an inter-institutional platform for interdisciplinary and multi-professional "case review" analysis and follow-up of cases, using a systemic approach.
   (c) Set up a national unit to combat cybercrime related to the exploitation of children, integrated into the child protection system.

7. Place prevention and education at the heart of public action:

   (a) Raise awareness among children, parents and professionals about digital risks and good practices.
   (b) Integrate a public-health perspective to assess the psychological and social impact of online violence.

3. Strengthen the detection of online violence and offences, as well as support and compensation for victims:

   (a) Reinforce mechanisms for detection and rapid intervention (i.e. strengthen the mechanisms of the BEE SECURE Stopline and the role of ALIA).
   (b) Ensure follow-up of reports and sanction perpetrators.
   (c) Create compensation funds and psychological and legal support services for victims.
   (d) Introduce mandatory specialised training for professionals responsible for assessing and managing situations of risk.
   (e) Provide support for people addicted to pornography.

Recommendations from the
OKAJU's 2024 annual report regarding

The protection of children from online violence and other harms related to digital tools

At the level of legal and regulatory developments

1. Update the Grand-Ducal Regulation of 8 January 2015 to better take social networks into account.
2. Include content creators as "new media" and establish specific terms of reference for them.
3. Introduce mandatory warnings and pictograms for sensitive content.

4. Implement age-verification systems effectively, for example through an age-verification system using LuxTrust.

5. Introduce legal age limits according to type of use: a minimum legal age of 3 years for exposure to screens, followed by gradual, age-appropriate exposure; a minimum legal age of 15 years for owning smartphones and other internet-connected devices and for using them without parental/adult supervision; and a minimum age of 16 years for using social media without parental oversight/supervision. Parental-control tools as well as safe, child-appropriate phones should be encouraged throughout childhood (following the example of Ireland and Australia, for example).

6. Implement a progressive system of gradual, step-by-step access to screen use and social media.

7. Pursue determined action at European level in order to raise and harmonise upwards the protection measures against online violence in all areas and levels of regulation.

8. Create in Luxembourg a supervisory and coordination commission for the prevention of and intervention against online violence against children.

At the level of strengthening mechanisms

9. Strengthen BEE SECURE by giving it more proactive means of action; although BEE SECURE is a strong asset with its helpline and stopline, these mechanisms remain insufficient because they operate *a posteriori*, and the virality of content on social media would require short-term and a priori regulation to be effective for vulnerable audiences.

10. Introduce follow-up for reports, which is currently absent due to the anonymity linked to the stopline.

11. Make the BEE SECURE helpline available 24/7.

12. Systematically train education and childcare professionals (on risks related to the digital world, monitoring tools, etc.).

13. Strengthen coordination between prevention and child protection services in the digital world and, in particular, link child protection services with cybersecurity services.

14. Guarantee that children who are victims of online violence receive psychosocial or psychotherapeutic care.

At the level of preventive action

15. Establish a public-health prevention approach for harms linked to children's use of digital tools, i.e. an integrated prevention approach encompassing primary, secondary and tertiary prevention.

    Examples of primary-prevention actions, aimed at avoiding the emergence of problems before they arise:

    - Introduce a legal age for owning smartphones and other digital tools as well as for using them without parental or adult supervision.
    - Develop attractive alternatives to digital activities (for example, free and supervised activities such as sports, cultural or artistic activities, board games, encouraging in-per-

son social interactions, creating age-appropriate leisure spaces, opening school playgrounds and sports halls to the public at weekends).
- Raise parents' awareness of "good practices" (limiting screen time via parental controls, supervision, etc.).

Examples of secondary-prevention actions, aimed at detecting and intervening early when problems start to appear:

- Train professionals (teachers, educators, etc.) to identify victims and perpetrators of cyberviolence and to carry out appropriate interventions.
- Promote rapid intervention in situations of risk.
- Develop peer mediation.

Examples of tertiary-prevention actions, aimed at reducing the consequences of identified problems and preventing reoffending:

- For victims: provide care for victims (psychological support, legal assistance) and reparation for the harm suffered.
- For victims' families: provide family psychological support, training on enhanced protection tools and support in legal procedures.
- For perpetrators: set up accountability programmes, behavioural therapies and support to help them understand the impact of their actions.
- For perpetrators' families: provide support in setting clear limits and responsibilities, help in establishing a strict framework, and psychological support where needed.

16. Promote child-appropriate secure mobile phones (basic mobiles allowing only calls and SMS, and mobiles with limited functions and built-in parental controls).

17. Implement fundamental principles and basic rules governing children's use of digital tools.

Mir si fir dech do!

Ombudsman fir Kanner a Jugendlecher
Défenseur des droits de l'enfant

65, route d'Arlon - L-1140 Luxembourg
contact@okaju.lu 28 37 36 35
www.okaju.lu - www.kannerrechter.lu

Oppassen
Nolauschteren
Agräifen