

Protecting children and older people without weakening encryption

A messenger from Berlin stops harmful messages before they reach anyone. No backdoor, no master key. Nobody reads along. Not even us.

THE DEBATE

Chat control presents a false choice

The 2022 Commission proposal (COM(2022) 209, procedure 2022/0155(COD)) is still under negotiation in the EU. At its core: child sexual abuse material and grooming.

Protection only with a master key?

Scanning in transit requires a backdoor or a central key that could open private chats. The question is not whether people are protected, but **where** the check takes place.

THE APPROACH · THE CHECK HAPPENS ON THE DEVICES

1 · Sender's device

The message is still in plain text. The app checks it for risky patterns before it is encrypted and can warn or stop the send.



2 · Transmission

End-to-end encrypted. The provider cannot decrypt or read anything in transit. Encryption remains fully intact.



3 · Recipient's device

After decryption the message is checked a second time before it is displayed. Two layers of protection, no reading in transit.

The sender sees which rule was broken. The message stays with them. **Neither a backdoor nor a master key** is needed.

WHAT IS DETECTED

Abuse

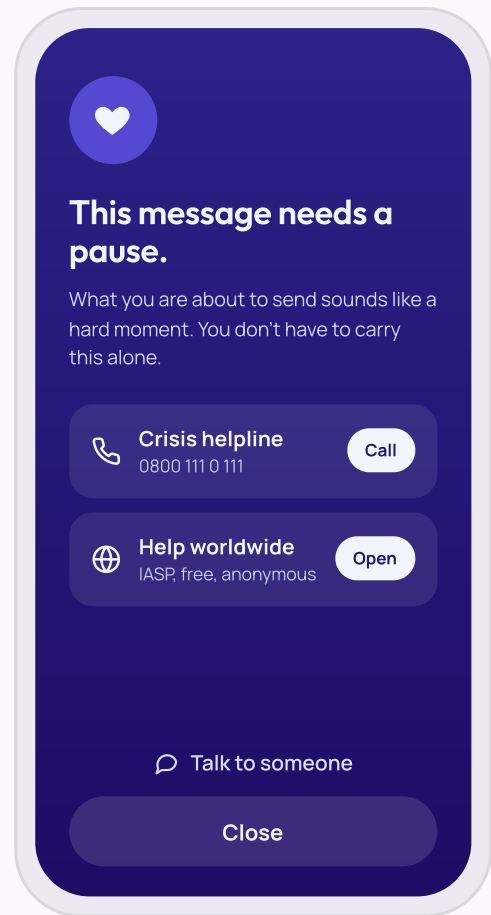
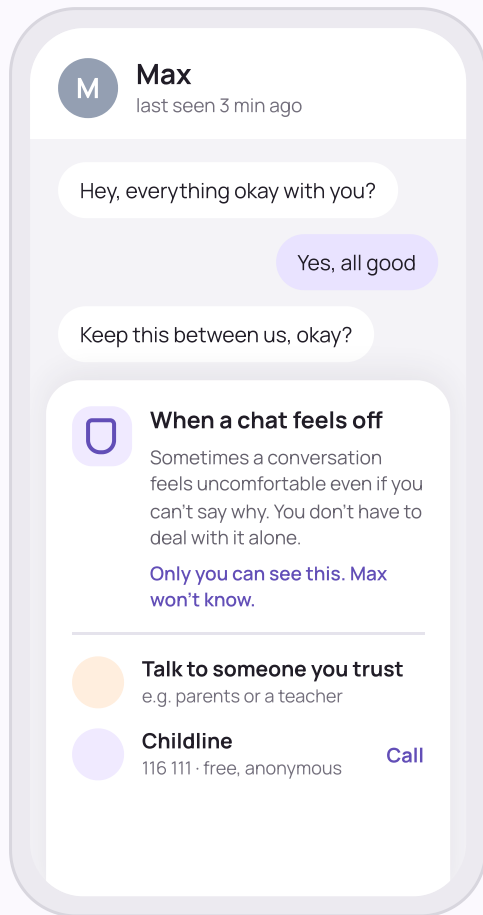
Hate Insults Threats Bullying
Grooming Unwanted images
Self-harm

Fraud patterns

Grandparent scam Links and URLs
Bank account numbers Phone numbers
Requests for money

The same mechanism protects **children** from abuse and **older people** from fraud. Warning and stopping happen on the device. The provider receives no content.

Two examples: grooming notice and self-harm



RECIPIENT

Grooming notice

The app detects the pattern on the child's device and places a calm help card over the chat. The sender is not notified.

SENDER

Self-harm

Before the message leaves the device, the app pauses and shows help right away. No blame, no reading along.

THREE LAYERS · PREVENTION, REPORTING AND LAW ENFORCEMENT WORK TOGETHER



Technical prevention

Checks on the sender's and recipient's devices. Harmful messages are stopped before they reach anyone.



Reporting function

Problematic content or contacts can be reported directly from the app. The same for children, parents and older users.



Interface to the BKA

Where required, cooperation with law enforcement authorities. Without access to encrypted communication.

€0

All core and safety features are free of charge.

Berlin

Developed and operated in Germany.

In conversation

With parents, schools and child protection organisations in several German states.



José Díaz · Founder, KindChat

jose.diaz@kindchat.app · presse@kindchat.app
kindchat.app/presse

sonrisa ventures GmbH · Kleiststraße 35 · 10787 Berlin
Berlin-Charlottenburg Local Court, HRB 150942 B
Managing Director José M. Díaz Delgado