Guidance from the Conference of Independent Data Protection Authorities

of the federal and state governments of April 29, 2021

(Status: April 29, 2021)

Use of digital contact tracing services

on the occasion of event, furnishing, restaurant and

Business visits to prevent the spread of Covid-19

1 Introduction

The conference of the independent data protection supervisory authorities of the federal and

Länder (DSK) in its statement of March 26, 2021 "Contact tracking in

Times of the corona pandemic - practical solutions with a high level of protection per-

Connect son-related data" already pointed out that digital processes

for the processing of contact and attendance data (hereinafter contact

tracking systems) must be operated in accordance with data protection regulations. The present

Orientation guide explains the requirements for such systems and their

drive resulting from the legal requirements. It is primarily aimed at

Developers and responsible persons i. S.v. Art. 4 No. 7 GDPR (see section 3).

In addition to the legally required tracking of contacts in

fected persons by the health authorities, systems are developed and operated

that take a different approach. They aim to inform people

about the risk of infection they are exposed to due to their proximity to an infected person.

goods and the responsible handling of this information. This

approach enables data-saving solutions that get by with pseudonymous data

and their security is not based on the trustworthiness of central systems.

rests. However, an exclusive implementation of this approach meets the current requirements

legal requirements do not. Should the legislature, however, digital solutions

permit the transmission of attendance documentation by organizers

not require the health authorities, then would be from data protection law

View solutions of this approach preferable.

2. Legal starting point

The data protection regulations to be fulfilled by those responsible (see Section 3)

technical requirements for the legally compliant processing of personal data

for digital contact tracing result from the General Data Protection Regulation

tion (DS-GVO), in particular from the principles of Art. 5 DS-GVO. So is for everyone

Processing requires a legal basis, it is the transparency of the procedure

ensure that the processing is appropriate for the purpose and to the necessary

to limit the amount (data minimization), to ensure the correctness of the data

afford to ensure a storage limit for this necessary purpose so-

how to ensure the integrity and confidentiality of the data throughout the process

afford.

Without prejudice to general federal law bases of contact data collection

According to Section 28a Paragraph 1 No. 17, Paragraph 4 of the Infection Protection Act (IfSG), the

Regulations for contact tracing in the individual federal states regarding

the contact data to be collected, with regard to the question of who and to what extent

Contact details must be collected in order to carry out contact tracing in the event of infection

to enable the health authorities, and with regard to the control of the

Contact details from the health authorities.

3. Spheres of Responsibility

Responsibilities within the meaning of Art. 4 No. 7 DS-GVO must be clearly regulated

be. Depending on the constellation of the procedure, those responsible can

be a service provider, an event organizer or a health authority. In the case of joint

responsibilities according to Art. 26 DS-GVO, it must be clearly regulated in advance which

expensive for which processing phase are responsible. So then z. B.

to specifically regulate who, according to Art. 13 DS-GVO, is responsible for the information obligation, the Right of future according to Art. 15 DS-GVO, the right to correction and deletion (Art. 16 and 17 DS-GVO), for the data protection impact assessment in accordance with Art. 35 DS-GVO and for personal data breach notifications Art. 33 DS-GVO is responsible. This must then be included in the agreement on the Joint responsibility according to Art. 26 Para. 1 DS-GVO specifically fixed in writing become. The obligations mentioned must also be included in the respective order processing contract i. s.d. Art. 28 Para. 3 DS-GVO are regulated.

4. Lawfulness of Processing

The processing of personal data is only lawful if it is the processing phase by the respective person responsible on a legal basis position can be supported. Therefore, the individual actors must be considered separately th:

4.1. service provider

For the implementation of the following processing steps, the service bidder responsible for data protection i. s.d. Art. 4 No. 7 GDPR. He can min- at least the following processing of the user's personal data – one subject to the relevant contractual agreement - based on Art. 6 Para. 1 Sentence 1 lit. b GDPR support:

- the registration for the use of the service with identifying information about the person concerned and the organizer,
- the storage of personal data in the end devices of the affected persons and
-

depending on the design, the transmission of contact details to the organizers in the course of attending an event, as well as

- the storage of data about encounters with other people on private

father meetings.

If the service provider transmits the data concerned at the request of an infected person

sucher history, it is a data transmission of health data

i. S.v. Art. 9 Para. 1 GDPR. The service provider can use this transmission on Art. 6

Paragraph 1 lit. a i. V. m. Art. 9 Para. 2 lit. a DS-GVO.

As far as the processing of the service provider in addition to contact tracking

also other health data, e.g. about Covid19 symptoms or test results

includes, the processing authorization required in this respect can only result from an

express consent of the data subject in accordance with Art. 6 Para. 1 lit. a, 9 Para. 2 lit.

a GDPR can be derived.

4.2. organizer

According to § 28a Abs. 1 Nr. 17 IfSG i. V. m. the Corona Protection Ordinance

regulations or laws of the countries to document the contact

animal and keep for the legally prescribed time. This duty can

depending on the regulation in the respective corona protection ordinance or law of the country

can also be met by digital documentation. As far as organizer

by law to collect contact data and to request their transmission

are obliged to contact the health authorities for the purpose of contact tracing,

they are considered by the legislature to be responsible for data protection

(§ 28a Para. 4 S. 1 IfSG in conjunction with the state law regulation). In this respect, there is

Art. 6 (1) sentence 1 lit. c and, if applicable, Art. 9 (2) lit

personal and possibly health-related and thus particularly

to process the data to be protected.

Do private individuals collect data from other natural persons who are contacted by them

organized gatherings such as family celebrations, this recording

2 (2) lit. c GDPR and therefore not

under the regulations of the GDPR. As far as the transmission of the personal

Data of the guests of the private meeting by the private individual to the competent

In the event of infection, the health department no longer falls under the household exemption,

it is in any case permissible according to Art. 6 (1) (c) and Art. 9 (2) (i) GDPR, insofar as

the private individual thus fulfills his legal obligations according to § 25 para. 2 i. V. m.

16 para. 2 IfSG.

4.3. health department

The legal basis for the processing of personal data by a

health office for contact tracing can be found in the Infection Protection Act (IfSG)

i. In conjunction with the corona protection regulations or laws of the federal states.

As soon as the processed data itself or the circumstances of the processing

treatment shows that data of an infected person is being processed - this is

This is especially the case if the infected person provides information about their stay

Events and facilities, as well as, if necessary, about encounters with others

persons in the private sector to the health department - is of a processing

processing of health data i. S.v. Art. 4 No. 15 GDPR. for the

Health Department, the permission to process this data results from Art. 6 Para. 1

lit. e, paragraph 3 lit. b, 9 paragraph 2 lit. i GDPR i. V. m. § 28a paragraph 4 sentence 4 IfSG.

5. Purpose and purpose limitation

§ 28a paragraph 4 sentence 3 IfSG establishes a legal, compared to general purpose

Change facts priority earmarking for the contact data processing

types of data specified by law.

The organizers, who are legally obliged to collect the data, are not allowed to use the contact data

process for a purpose other than delivery to the health authorities,

§ 28a paragraph 4 sentence 3 IfSG. A transfer of the transmitted data by the health

health authorities or further use by them for purposes other than the

Clock tracking is also excluded, § 28a paragraph 4 sentence 6 IfSG. As far as that

Service provider works on behalf of event organizers or health authorities

further processing of the contact data for other purposes outside of a

the customer is not permitted. As far as the service provider in advance of the data

survey by the organizers or as part of a joint responsibility

tion works on his own responsibility, he is also obliged to apply the regulations of the

§ 28a para. 4 IfSG without prejudice to the question of a viable processing

authorization to process for other purposes as well as the other actors

resists.

Due to the strict legal regulations, anonymization of the

Contact data with a view to later evaluation for purposes other than

Contact tracing not allowed.

6. Ensuring the voluntariness and preservation of

Privacy Policy

6.1. voluntary

The use of digital contact tracing services by data subjects

should be voluntary to reduce the risk of discrimination when participating in the

to avoid social life and a high willingness to cooperate

promote.1

A voluntary decision for an application requires a high degree of transparency

ahead, so that the visitors who use them are informed

can make a decision.

Voluntariness presupposes a choice. The DSK welcomes the large number of

bidder, which offers the obligated and data subjects the opportunity to choose between

to choose from different services. In addition, affected persons should

always have the opportunity at events where contact details

must be processed according to infection protection law, contact details without

a suitable own end device, without entering into a contract with a provider

and without giving consent.

When questioned by the health department, the person concerned can

Refuse to respond to such questions, the answer to which you yourself or one of the

Section 383 (1) nos. 1 to 3 of the Code of Civil Procedure

driving criminal prosecution or proceedings under the Ordinance Act

would expose breaches of law (cf. Section 25 (2) in conjunction with Section 16 (2) sentence 4 IfSG). There-

fro the operator of the system must ensure that the data that a

affected person saved as part of their own visit and contact history

1 “The systematic and comprehensive monitoring of the site and/or contacts between natural

people is a serious invasion of their privacy. This is only legitimate if the user

App used voluntarily for each of the intended purposes. Conversely, this means that people who

do not want to or cannot use such apps, no disadvantages may arise."

shot: Guidelines 04/2020 for the use of location data and contact tracing tools in combination

related to the outbreak of COVID-19, https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guide-

lines-042020-use-location-data-and-contact-tracing-tools_en

only after approval by the person concerned to the health department

and the user has previously had the opportunity to use this information

to make a choice.

6.2. Transparency of data processing

Service providers and organizers as well as the health authorities must, insofar as they

are each responsible for processing, the data subjects in accordance with

of the legal requirements of Articles 13 and 14 GDPR. As far as that

If the organizer is responsible and the provider is the processor, the latter must

provide the organizer with all necessary information so that

terer of his obligation to inform according to Art. 13 DS-GVO towards the visitors after

(Art. 28 para. 3 sentence 2 lit. e GDPR).

The data subject must be informed as to who is responsible for the

processing is responsible under data protection law, on which legal basis

location of the processing and what rights you are entitled to. For the person concerned

In this way, it must be clearly recognizable who is responsible

to assert their rights and who can act as a processor for

the security of the personal data is guaranteed. According to Art. 13 Para. 1 lit. a and

c DS-GVO, users of digital contact tracing services must in particular

be informed about which actor for which processing – specified according to

their processing purpose – is responsible. This information must be in a precise, trans-

parenter, understandable and easily accessible form as well as a clear and

use simple language.

It would therefore be best for the person concerned to have a central contact point that

gene of the data subject to the respective person responsible.

Finally, digital solutions offer a simple way of fulfilling internal

to facilitate information obligations according to Art. 14 DS-GVO for the health authorities.

If contact details actually have to be transmitted in the event of an infection, we can

data subjects in contrast to general advance information (Art. 14

Para. 5 lit. a DS-GVO) will be specifically informed of this directly via the app.

This opportunity to ensure transparency should be taken into account when designing

services are not left unused.

6.3. Confidentiality, minimizing the accessibility of the data and

earmarking

To ensure the strict earmarking, technical and organizational

toric measures that are excluded from the services or with

personal data processed with their help for purposes other than those specified

purposes can be further processed.

In order to ensure this earmarking as well as the confidentiality of the contact

ments, it must be established and enforced that only the competent authority

health authority has access to the respective personal data. This may

in the case of questioning the infected person according to § 25 para. 2 i. V. m. 16

Para. 2 IfSG only with the participation of this person (see above) and in the case of handing over

the contact details i. S.v. § 28a paragraph 4 sentence 3 IfSG only with the participation of the organizer

be made possible. If a time or location-based restriction of the

contact data to be transmitted is required (e.g. contact data of all persons of a

room in which an infected person was staying), the service should have a restriction

provide on this data. The principle of data minimization (Art. 5 Para. 1 lit c

i. V. m. Art. 25 Para. 1 DS-GVO) is in the planning phase for the technology design

already to be observed (data protection by design) as in operation.

According to § 28a paragraph 4 sentence 2 IfSG, those responsible have to ensure

that acknowledgment and further processing of the recorded contact data

unauthorized persons or institutions is excluded. In connection with Art. 32

DS-GVO results in the organizers having at least the identifying information

event-related already during the survey (i.e. according to organizers and times

separately) must be encrypted in such a way that they can be

ments that only the respective data subject and the responsible health

offices are known, not decrypted and different stays and the

same person are not connected to each other through the identifying information

can be brought.

The assignment of the contact data to an identified or identifiable natural

person may only be given to a competent health authority in the course of follow-up

the contacts of an infected person are made possible. That means in particular

dere that neither the organizers nor the service provider a decryption

may be possible. Holding a master key for the decryption of all

Records contradicts this requirement.

7. Rights of data subjects to rectification, erasure

and information

Those responsible are required to ensure that the processing of data subjects

applications can be made in accordance with the legal requirements. prerequisite

The first step in processing is the granting of data subject rights.

processing of data subject applications, the identification of the data subjects. The need

identification does not authorize the processing of additional data. Provide one

data subject to provide the data required for identification in the individual case

tion, applications from data subjects must be processed further (EG 57 S. 2 of the GDPR).

If those affected do not do this, in accordance with Art. 11 Para. 1, Art. 12 Para. 2

S. 2 DS-GVO data subject applications are not processed further.

If the personal data is pseudonymised by the responsible

are kept mismanaged, affected applications must be processed if

these as part of the identification process of their own accord

provide the pseudonyms under which the data is stored in the system

become. It must be ensured that the pseudonyms are generated and used in such a way

be protected that this does not lead to unauthorized disclosure, correction

or deletion by means of guessed or unauthorized pseudonym identifiers

can be turned.

This also applies if several actors have to work together to grant rights

senior

7.1. Right to correction according to Art. 16 DS-GVO

Precautions must be taken to ensure that affected persons are informed immediately

the correction of incorrect information about your person or about a stay in

of an event.

7.2. Right to erasure in accordance with Art. 17 GDPR

The person responsible must ensure that, on the one hand, the contact data is stored in the system

automatically after expiry of the statutory retention obligation

be deleted and on the other hand that all personal data of the user

Zers, who are not responsible for compliance with a legal obligation in

as part of contact tracing, will be deleted if this

no longer wish to use the service. The data will not be recovered from the deletion

summarizes, for which there is still a legal storage obligation.

7.3. Right to information according to Art. 15 DS-GVO

The data subject has the right to obtain confirmation from the person responsible

to request whether and which personal data relating to them are processed

and to receive a copy of this data (Art. 15 DS-GVO).

8. Technical and organizational measures

Basic requirement for the operation of contact collection services

form secure data processing systems. According to Art. 32 Para. 1

DS-GVO the state of the art, the implementation costs and the type of

fang, the circumstances and the purposes of the processing as well as the different

Probability of occurrence and severity of the risks associated with processing

kens for the rights and freedoms of natural persons. It has to be

level of protection appropriate to the risk must be ensured, i.e. the selection of the security

Security measures are based on the specific processing activities and the associated

associated dangers to the rights and freedoms of those affected.

Data protection must already be given sufficient consideration in the conception phase.
found and in particular the principles of the processing of personal data
Guarantee data according to Art. 5 DS-GVO (cf. Section 2, Para. 1 of this orientation
aid). In this respect, the person responsible is obliged according to Art. 25 DS-GVO,
at the time of determining the means of processing as well as at the time
technical and organizational measures suitable for the actual processing
to implement.
In the context of this guide no comprehensive technical
Test criteria are defined, but the following will explain which ones
Requirements for contact tracing systems the Conference of Independents
Federal and state data protection authorities with regard to technical and organizational
organizational measures and their implementation for compliance with data protection
principles and the protection of the rights of those affected as appropriate. The criteria
are then supplemented by best practice tips.
A possible methodology for the implementation of these requirements contains the standard
Data Protection Model (SDM).2

8.1. Privacy by design and privacy-friendly presets

Pursuant to Art. 25 (1) and (2) GDPR, those responsible must ensure that they
Plan and design procedures already in compliance with data protection (data protection through
technology design) and also with data protection-friendly default settings.
ben. The principle applies here that default settings (e.g. an app for
Contact data collection) only data that is required for the specific processing purpose
are required to be processed (principle of purpose limitation, Art. 5 Para. 1 lit b
GDPR). This obligation applies to the amount of personal data collected
data, the scope of their processing, their storage period and their accessibility. The-

This behavior must be ensured without user intervention.

When developing contact collection services, it is important to ensure

that already in the planning phase of a development process concerns of data

protection and taken into account when designing the processes.

Are further contact tracing systems used that are not based on contact tracing

tion-oriented functions are integrated, these may be used under data protection law

essential properties of the system and in particular

this integration does not lead to higher risks. Art. 25 Para. 2 DS-GVO (data

protection-friendly defaults) requires that such functionalities only

2 https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

may be activated if they have been expressly activated by the data subject

the.

8.2. Risks of central data storage

In the development of contact tracing services, it can generally be

A distinction can be made between two different approaches: On the one hand, the group of

Services that store the contact details of the data subjects in a central server

Deposit infrastructure, and on the other hand services that store the data as far as possible

initially kept decentralized, i.e. on the end devices of the persons concerned and the

Save organizer.

Both approaches basically allow the same functionality, both in terms

on the fulfillment of the infection protection requirements according to § 28a paragraph 4

IfSG, as well as compliance with data protection regulations, which in

section 5 to 7 of this guide. Both approaches require

also central services and systems that provide these functionalities.

When deciding to implement one approach or the other

consider the risks that come with it. A compromise of the central

ral services and systems by unauthorized third parties who are associated with a violation of the confidentiality and integrity of these services and systems can be too special lead to high risks if these systems are not only used to control processing, but also for the extensive storage of sensitive data about the recording of people in institutions and their participation in events be turned.

In principle, these risks can be countered with encryption. In this case is to consider where the keys are stored, who is in control possesses these keys and how they are obtained through unauthorized actions or can be used. A decentralized storage of the keys represents a meaningful full risk-reducing measure. However, it is itself weakened if the tools used for key management by the centrally operated system systems are made available and unauthorized persons can gain control of these systems teme can be manipulated.

The service providers are obliged before starting the operation of the service, the to analyze in detail the effects of the model you have chosen and its effectiveness of the planned measures.

8.3. security of processing

For contact tracing systems that process contact data on a large scale ten, the risk to the rights and freedoms of individuals by appropriate to contain technical and organizational measures effectively. a data protection-impact assessment can serve to determine the effectiveness of technical and organizational measures to protect personal data.

It is either to be carried out by a responsible person according to Art. 35 DS-GVO, if the personal data processed by him is likely to become one result in a high risk of rights and freedoms, or can be voluntarily

t providers for many, especially small, responsible persons are carried out. Consists
an obligation to prepare a data protection impact assessment, this is
to complete the processing. A data protection impact assessment should
be carried out as early as possible in the planning and development process, since
with which the findings can flow back into the development.
When selecting the technical and organizational measures, particular
to note the following:
 Data transfers to third countries or international organizations without
adequacy decision of the EU Commission are associated with additional risks
connected and may prove to be inadmissible if the specifications of the
Chapter V of the GDPR are not complied with. It is particularly recommended
the use of data centers in the spatial scope of the
GDPR.
 Measures to implement the principle of data minimization are to be taken
cause.
 Applications and systems must support the entire period of use
Vulnerabilities and other bugs are updated in a timely manner, in case of critical ones
vulnerabilities immediately.
 Principles of IT security must be observed. Confidentiality, internal
Integrity and availability of the data must be guaranteed at all times. This around
summarizes all data processing and thus applies to both stored
data as well as for actively processed data. Measures to ensure that
These principles include:
o Subsequent changes to contact details should, if at all
permissible, comprehensible and should be versioned.
o Central trust anchors (e.g. a PKI) lie with a trustworthy

external agency.

o The key creation of the user certificates should be done locally on the

advice is given if this is reasonably possible.

O

Identifiers, pseudonyms and keys should be used at short intervals

be changed in order to create a profile over longer periods of time

to complicate.

o The authenticity of the remote station should be verified by all

communication involved must be verifiable.

o The transmission of the individual contact data collection entries as

further processing via other actors must also have encrypted

Rare connections are made so that third parties are not aware

can take the contact details.

o The retrieval of the health authorities must be based on health authority-specific

visual certificates.

o Access by the health authorities must be logged. Protocol-

data must be protected against unauthorized access.

o Transmissions of contact data are in addition to content encryption

transmission encryption in compliance with the BSI TR

02102-2 or others that are equally effective according to the state of the art

Measures to secure in order to also protect metadata on the transport route

protection.

o The procedure should provide adequate protection against identity

custom at the expense of the persons concerned and against the entry of

attendance data that do not correspond to an actual stay,

exhibit.

o Data that is no longer required for the fulfillment of the purpose

be safely deleted. This also applies to services that are no longer required

versions and copies of data.

o Access for maintenance and administration of systems and

Services critical to the operation of the contact tracing system

table, or for authorization of contact data retrieval

secure authentication (e.g. two-factor authentication)

required according to the state of the art.

o Measures to implement the principle of data minimization

are to be arranged.

o As far as identifying within the contact tracing system

Information must be checked before it is accepted, this check must be carried out

be protected against manipulation.

o A processing of metadata (including traffic data) must

be limited to what is necessary and there shall be no linkage

with contact details.

 Apps for recording contact data must not transmit any

make personal data to third parties and in particular

do not include tracking and analysis services.

 When using external service providers, it must be ensured that

that through this no usage data - outside of the required

Provision of the contractually agreed service - for other purposes

cke (telemetry data, data to improve the service, diagnostic data

ten, etc.) are processed without a sufficient legal basis.

8.4. Best Practice Advice

Observing the following data protection best practice information serves

the protection of the rights and freedoms of the persons concerned, without other interests to interfere with eating.

- The service provider should, as far as possible, simply provide usable functions with which they can who can assert or implement the rights. In particular, responsible corrections (cf. point 7.1) not make themselves, but can use the service to provide the data subjects with the technical option make it possible to independently correct incorrect data after it has been collected, insofar as this is done without breaching the confidentiality of the stored data can happen and the integrity of the residence documentation (e.g. through versioning of the entries) remains unaffected.
- The service provider should inform data subjects, organizers and health make applications available to security offices, the integrity of which is guaranteed by nature test can be verified.
- In order to increase the acceptance of the applications, the interested Public information about the technical measures that the responsible verbatim to ensure data protection-compliant processing fen, are available to the extent that the publication itself does not leads to security risks. This also includes the publication of the source Codes of the respective applications, the persons concerned, organizers, use bidders and health authorities. To enable verification, should reproducibility of the published binaries be possible.
- Mobile apps should also be offered on distribution platforms that are not are under the control of the major mobile operating system vendors since to justify the use of the platforms of these providers with additional connected to the data processing.