

Data protection information

Accreditation with reliability check on the occasion of the

Charlemagne Prize Award Ceremony in Aachen on 09. May 2024

Dear Ladies and Gentlemen!

The Charlemagne Prize ceremony is an important event. We thank you for wanting to be part of it and look forward to working with you.

A peaceful, trouble-free course of the event is in the well-understood interest of all participants. In order to ensure this, we only wish to grant access to the event venues to persons who have been accredited for this purpose.

1. data collection and processing by the organiser

Since the accreditation procedure inevitably involves the processing of your personal data, which can only take place on the legal basis of your express consent, you will receive information below about what happens to the information you provide on the application form.

Your personal data is collected, processed and used via an accreditation system. The data collected within the scope of the accreditation procedure is electronically recorded and stored on a server of the State Office of Criminal Investigation in Düsseldorf. The data is transmitted exclusively via secure transmission channels.

All personal data stored in the organiser's accreditation system will be deleted three months after the end of the event if accreditation is granted and twelve months if accreditation is refused. This retention period is intended to ensure qualified processing of enquiries about your own stored personal data and enquiries or complaints about accreditations that have been granted or not granted.

The data provided by you in the application form will be processed and used by the organiser exclusively for the purpose of deciding on the granting of the right of access and its scope and for monitoring compliance with the relevant restrictions. Your data will not be accessed by third parties or passed on for other purposes. The collection, processing and use of personal data thus serves to guarantee the security of the event.

All organisations involved shall ensure that the aforementioned provisions are complied with.

If you wish to assert your data protection rights in accordance with §§19,20 BDSG or §§ 18, 19 LDSG NW (in particular rights of access and rectification), please contact the office responsible under data protection law. These are the organisers:

Stiftung Internationaler Karlspreis zu Aachen

Geschäftsführer: Mag. Bernd Vincken

Fischmarkt 3

52062 Aachen

Telefon: 0241/ 401 7770

E-Mail: vincken@karlspreis.de

Stadt Aachen

Oberbürgermeisterin Sibylle Keupen

Rathaus/ Markt 38

52062 Aachen

E-Mail: oberbuergmeisterin@mail.aachen.de

Pontifikalamt

Domkapitel Aachen

Dompropst Rolf-Peter Cremer

Klosterplatz 2

52062 Aachen

Direktorium der Gesellschaft für die Verleihung des internationalen Karlspreises

Vorsitzender: Dr. Jürgen Linden

Kasernenstr. 24

52064 Aachen

E-Mail: info@ra-juergenlinden.de

2. background check

Within the framework of the accreditation of all persons of the security services as well as persons who are active in the security areas of the event, it shall also be checked whether the security authorities involved have knowledge which, from their point of view, would stand in the way of an admission to the respective venue (background check).

For this purpose, an extract from the data collected with the declaration of consent (surname, first name, maiden name or former names, date of birth, place of birth, gender, nationality as stated in the ID card, postcode, city, street, house number, federal state, country, type and number of the ID card, name of the event, function at the event, registration number) shall be made available electronically to the security authority Police Headquarters Aachen as the "Central Office" for the purpose of conducting a background check.

The security authorities Landeskriminalamt NRW (North Rhine-Westphalia Criminal Police Office) and Polizeipräsidium Aachen (Aachen Police Headquarters) use the data to check whether there is

anything stored about you in the files of the police forces of the federal states and the federal government that would conflict with your deployment for reasons of security.

If there are any findings that make an extended enquiry of your data with other authorities appear necessary, your data may also be forwarded to the responsible state criminal investigation offices, the BKA, the Federal Police, the Customs Criminal Investigation Office and the Federal Office for the Protection of the Constitution for review.

The results of all checks are sent separately to the Aachen Police Headquarters security authority as the "Central Office". The "Central Office" collates the results and provides feedback to the organiser as to whether information about you is stored in accordance with the following criteria.

2.1 Files used for the check

2.1.1 Police data

Your data will be checked against various police files that are kept by the police stations for the purposes of danger prevention and criminal prosecution. These are files that are used jointly by the federal and state police forces (composite files), but also files that are used separately by the federal and state police forces.

These are, in particular, so-called criminal offender files, in which criminal convictions, but also pending and discontinued investigations as well as criminal proceedings without a court conviction are stored, such as state protection files (these contain data on criminal offences with a political background or the membership of organisations or associations banned in Germany, etc.).

The duration of data storage in these files is determined by the provisions of the federal and state police laws. It is based on the individual case, taking into account the seriousness of the offence and, if applicable, the court decision, as well as on whether the person concerned was a juvenile (younger than 18) or an adult (older than 18) at the time of the offence.

As a rule, the retention period for felonies and certain serious offences as well as other nationally significant offences is ten years for adults, and five years for medium-level offences for adults and juveniles. In cases of minor importance, the review periods are reduced to three years. If a new relevant offence is stored for a person before the expiry of the storage period, the storage period may be increased as far as legally possible, while at the same time retaining the findings stored up to that point.

It is expressly pointed out that the information in the police files may be more extensive than in the Federal Central Register because, in principle, proceedings that have been discontinued by courts/prosecution offices or ended without a conviction may also be stored.

2.1.2 Data from the Office for the Protection of the Constitution

When being checked by the constitution protection authorities, your data will be compared with a joint file of the constitution protection authorities. The reasons for and the duration of storage in this file are determined by the federal and state constitutional protection laws. As a rule, the storage period is five years for minors and ten or fifteen years for adults after the date of the last relevant information stored.

2.2 Criteria that are decisive for the decision ("catalogue of criteria")

The objective of the background check is to ensure the safe and trouble-free running of the event.

The aim is to prevent persons from working in security-relevant areas where it is to be feared that they could pose a risk to the event as a whole.

For this reason, the central office will report back to the organiser in the following cases that **police information** is available on you:

The files show legally binding convictions for crimes committed

- (offences punishable by a minimum of one year's imprisonment or more)

or

- misdemeanours (offences for which the statutory minimum term of imprisonment is less than one year or which are punishable by a fine) which, in individual cases, are of a nature or severity particularly likely to disturb the peace under the law, insofar as they are directed against the life, health or freedom of one or more persons or against significant property or assets belonging to third parties, are committed in the fields of illicit traffic in weapons or narcotics, counterfeiting of currency or stamps or are committed on a commercial, habitual, serial, gang or otherwise organised basis

or

- state protection offences

If you have been convicted several times by a final court decision for offences other than those of considerable importance, the police will inform the organiser of this if it seems appropriate after a careful examination of all the circumstances.

The same applies if other information about you is available, e.g. about ongoing or discontinued preliminary proceedings or criminal proceedings without a court conviction, or if there is information about state protection or narcotics or information from the area of organised crime which suggests that you will commit such offences in the future.

The authorities for the protection of the constitution will generally inform you that they have knowledge about you if there are actual indications that

- 1.

the applicant will commit acts of violence,

- 2.

the applicant has committed one or more acts of violence in the past which, by their nature or severity, are likely to disturb the peace under the law,

- 3.

the applicant belongs to or strongly supports a violent ideology,

- 4.

the applicant will call for acts of violence or has called for such acts in the past. The same applies if there are actual indications that the applicant is in danger of committing extremist propaganda offences or other acts with an extremist background which are likely to endanger/ damage public security or foreign interests or Germany's reputation.

As a matter of principle, the Federal Intelligence Service will notify the organiser that there are findings about you in the data files on international terrorism or organised crime which provide actual indications that

1. the applicant will commit acts of violence,
2. the applicant has committed one or more acts of terrorist violence abroad in the past, the nature and severity of which are likely to disturb the peace under the law,
3. the applicant is a member of a violent group abroad or strongly supports such a group,
4. the applicant will call for acts of violence or has called for such acts abroad in the past. The same applies if there are actual indications that the applicant is in danger of committing terrorist or other extremist acts which could endanger/damage public security or foreign interests or Germany's reputation.

2.3 Procedure

It is expressly pointed out that the police will only inform the organiser of the result of their reliability check. The reliability check serves as the basis for the organiser's decision on your accreditation or non-accreditation:

- If the check of your data by the security authorities shows that, in terms of the aforementioned criteria, there are no entries, this will be communicated to the organiser.
- If the examination by the security authorities reveals that, in accordance with the aforementioned criteria, there are entries concerning your person, this will be communicated to you and the organiser (without giving reasons). Such findings, in addition to other factual/professional reasons, can lead to accreditation not being granted.

If accreditation has been refused, you may raise your objections with the organiser.

If the organiser rejects your accreditation due to findings of the security authorities, your submission will be forwarded to the rejecting security authority(ies) via the Central Office, if applicable. Your objections will be examined and the notification to the organiser corrected if necessary.

You can assert your other data protection rights (in particular the right to information and the right to correction), as far as data processing by the security authorities is concerned, with the security authority named in the notification to you. To exercise your data protection rights, you can also contact the competent data protection authority of the respective Land or the Federal Commissioner for Data Protection and Freedom of Information, as well as the Data Protection Commissioner of the BMUB.

The data collected in connection with the background check will be stored by the aforementioned security authorities for a period of three months from the official end of the event in order to be able to determine retrospectively, if necessary, which findings were relevant, and then deleted. Until deletion, the data is blocked for general access. If there are findings according to the catalogue of criteria, the data will be deleted twelve months after the official end of the event.

3. voluntariness of your information

It is your free decision to fill in the application form and to give your consent to the data processing presented here, in particular to the background check. However, if you refuse to do so, accreditation cannot take place.

You also have the right to revoke your consent at a later date. In this case, however, any accreditation granted up to that point would have to be withdrawn. Your data will then remain stored in the accreditation database for a period of three months to enable qualified processing of enquiries.

If the background check at the security authorities has already been carried out at the time of the revocation, this would have no influence on the further storage of your data there until the expiry of the above-mentioned periods.