# PEMEA

# GDPR CONFORMANCE STATEMENT

PEMEA allows applications to roam across borders. How is data protection ensured? This document explores how PEMEA complies with the GDPR.

# PEMEA GDPR Conformance Statement

**Version:** 1.0

**Publication date:** 25/05/2020

**Status of the document:** APPROVED

**Authors that contributed to this document:**

This document was written by members of EENA.

**Authors:**

James Winterbottom - Deveryware

**Contributors:**

Bertrand Casse – Deveryware

Cristina Lumbreras - EENA

Luca Bergonzi – Beta80

Rose Michael - EENA

EENA

European Emergency Number Association

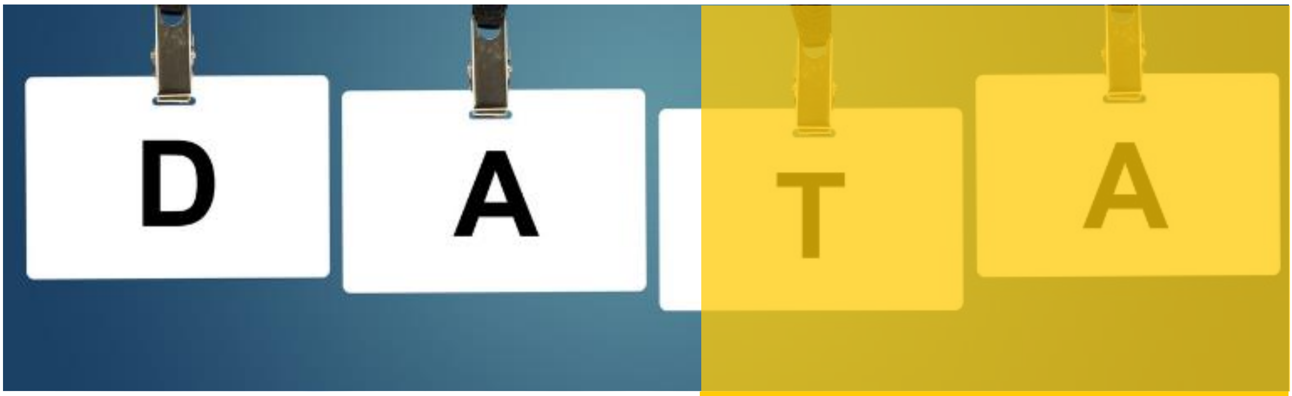
EENA 112

Avenue de la Toison d’Or 79, Brussels, Belgium
T: +32/2.534.97.89
E-mail: info@eena.org

**LEGAL DISCLAIMER:**

This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.

This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.



# EXECUTIVE SUMMARY

**PEMEA is the Pan-European Mobile Emergency Application framework. It enables any application to roam across Europe and provide accurate location and user information, as well as advanced communications services, for example, for people with language, vocal and hearing disabilities.**

The general operation of PEMEA requires some potentially sensitive information to be conveyed from the source application through a number of PEMEA nodes and ultimately to the destination Public Safety Answering Point (PSAP).

This document defines what information PEMEA entities may be privvy to and the restrictions placed on them in how they store and use that information.

In the framework of *General Data Protection Regulation* (GDPR)[1], this document describes the PEMEA entity functions in GDPR terms of Data Controller and Data Processors and what functions are performed by each component. In conclusion, this document identifies how PEMEA conforms with the edicts encompassed in GDPR and where responsibilities for access to, and storage of, specific information lie.

**PEMEA enables any application to roam across Europe. In doing so, some potentially sensitive information needs to be conveyed from the source application.**

**This document describes the PEMEA entity functions in GDPR terms and identifies how PEMEA conforms with the GDPR principles.**

[1] *https://eur-lex.europa.eu/eli/reg/2016/679/oj*

# 1 | PEMEA ARCHITECTURE OVERVIEW

**The PEMEA architecture identifies the different functional entities, their responsibilities and the necessary interface reference points to support emergency call-capable applications. This allows them to roam anywhere across Europe and potentially around the world. The PEMEA functional architecture is described in the *ETSI PEMEA specification TS 103 478*[2].**

The architecture defines five (5) primary entities:

1. The Application (App) that runs on the smart device.
2. The Application Provider (AP) is a server that talks to the App and converts its data into PEMEA messages.
3. The PSAP Service Provider (PSP) that provides interconnection between the wider PEMEA network and one or more PSAPs.
4. The Public Safety Answering Point (PSAP) where the user's call is handled and where the application data is ultimately sent.
5. The Aggregating Service provider (ASP) that brokers PEMEA messages between PSPs.

The architecture also defines four key reference points:

1. Pa, between the App and the AP. PEMEA does not define what messages are exchanged or over what protocol, it does, however, put a minimum set of requirements on the data to be provided.
2. Ps, between the AP and the PSP. Messages over Ps are always initiated by the AP towards the PSP. This interface is heavily defined and must be adhered to.

[2] *https://www.etsi.org/deliver/etsi_ts/103400_103499/103478/01.02.01_60/ts_103478v010201p.pdf*

3. Pp, between the PSP and the PSAP. PEMEA doesn't tightly define this interface though it does leave the option open for this interface to use the standard PEMEA signalling messages thereby having a "PEMEA-PSAP". Both the PSP-based and PEMEA-PSAP cases are covered by this document.
4. Pr, is the roaming interface, nominally between the PSP and an ASP, but may also be between two PSPs. This interface is the only bi-directional interface in PEMEA: PEMEA messages may be initiated in either direction.

While the basic definition described above meets a very minimal function set, in practice there are two other reference points not defined in the functional architecture but are still alluded to in the *ETSI PEMEA specification TS 103 478*.

The first of these reference points is described in Annex C of the *ETSI PEMEA Specification* and describes how the AP may advertise additional capabilities to the PSAP and how the PSAP may invoke these, but there is no reference point shown between the PSAP and the AP in the basic architecture. The PSAP invokes these capabilities in the AP by using what are referred to as "Reach-Back" URIs. Since Pr is already used in PEMEA, this document defines the capability invocation reference point between the PSAP and the AP as the PEMEA Capabilities reference point, designated Pc.

The trust anchor for PEMEA is called the PEMEA registry and is described in an overview in the *ETSI PEMEA Specification*. Since the information in the PEMEA registry is critical to the security and trust model of PEMEA, an explicit reference point between the PEMEA entities and the PEMEA registry is also required. In this document, the reference point between the PEMEA entities and the PEMEA registry is referred to as the PEMEA Entity reference point and designated Pe.

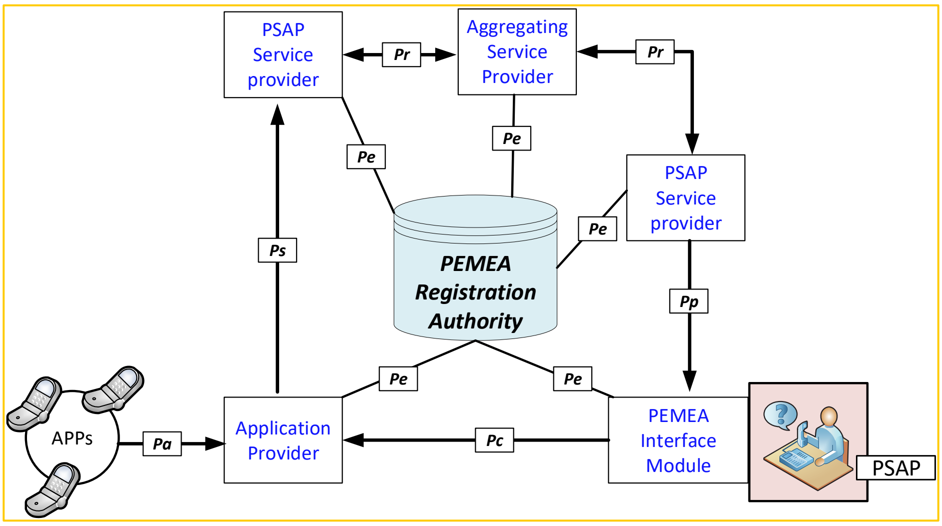


*Figure 1: Modified PEMEA architecture*

# 2 | ACCESS TO DATA IN THE PEMEA MODEL

**The AP is part of the Application Server provider domain. It initiates communication through the PEMEA network, the data processing components and ensures that personal data is only ever communicated between data controllers.**

The PSAP or terminating-PSP is always deployed inside the PSAP Authority domain and all data storage and access is done under the control and authority of the PSAP governance. The PEMEA PSAP or terminating-PSP is considered a data controller.

A non-terminating PSP may reside inside the PSAP authority domain so that they can manage the routing aspects internal to the PSAP authorities network, making it part of the data controller, or may it reside in the wider PEMEA network. In this latter case, it is considered part of the data processor.

The ASP is part of the data processor and interconnects multiple PSP and ASP instances.

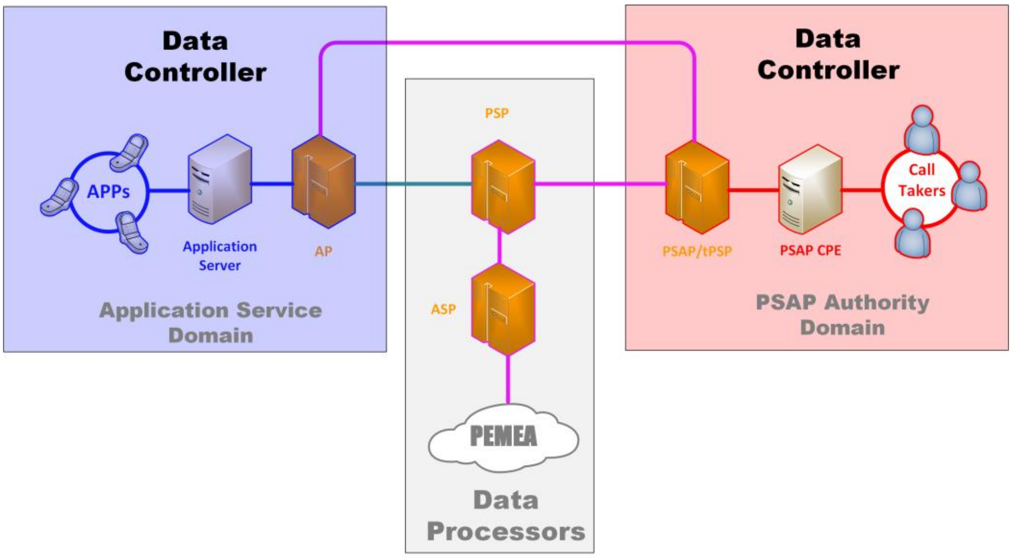


*Figure 2: PEMEA Data Controller Data and Data Processor model*

# 3 | PEMEA DATA ACCESS CONTROLS

**PEMEA mandates that each entity identify itself before accepting a connection and before passing data over a connection. This identity is qualified in several ways:**

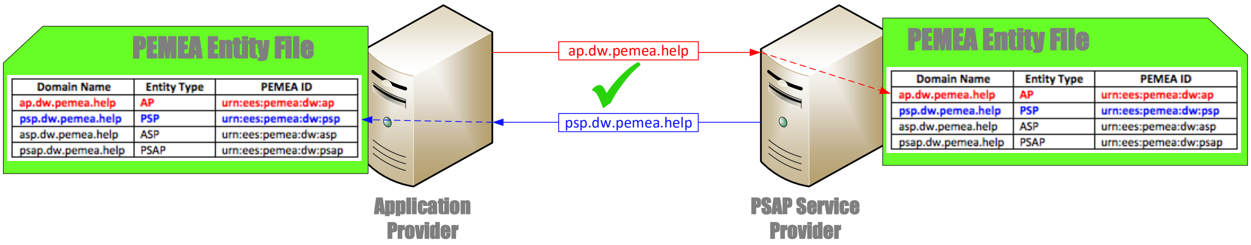
- Use of Client-side and Server-side security certificates that assert the ownership of a specific Internet domain name.
- The domain name certificate may be associated with only one PEMEA node.
- The PEMEA entity list provided by the PRA contains an entry for that domain name and defines the node type.
- The combination of valid domain and corresponding entity-type determines if the type of connection is allowed and hence what data is able to be accessed.

No entity must ever attempt to connect to an entity not in the PEMEA entity list. The PEMEA entity list is fetched from the PRA and loaded into each PEMEA entity at least once every 24 hours to ensure that the list of valid entities is up to date.

There are restirctions on which entity types may connect to each other and these are described in the following sections. The entities in each of the diragrams have already fetched the current entity list from the PRA over the previously described Pe interface.

## 3.1 | AP CONNECTIVITY

**The AP may only initiate connections to a PSP and it must have a direct relationship with this PSP; this is referred to as the sponsored PSP. If the neighbour PSP is not found in the PEMEA entity list, then it shall not initiate a request to it and the application will be notified that the message cannot be sent.**



PEMEA Entity File

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

PEMEA Entity File

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

*Figure 2: AP authentication to the PSP*

It is recommended that an AP always set the onErrorPost (defined in section 11.1.3 of TS 103 478) and onCapSupportPost (define in section 11.1.4 of TS 103 478) attributes in an EDS message. This means that the AP will always expect an answer. That answer may be an error or it may be an indication that the message safely arrived at the correct PSAP.

An AP will accept connections from any entity in the PEMEA entity list, except if the entity type is an AP. If an AP determines that the connecting entity is another AP, it will reject the connection.

An ASP or PSP may connect to the AP to send an error message indicating that the message could not be delivered. An AP rejects any message from an ASP that is not an error message.

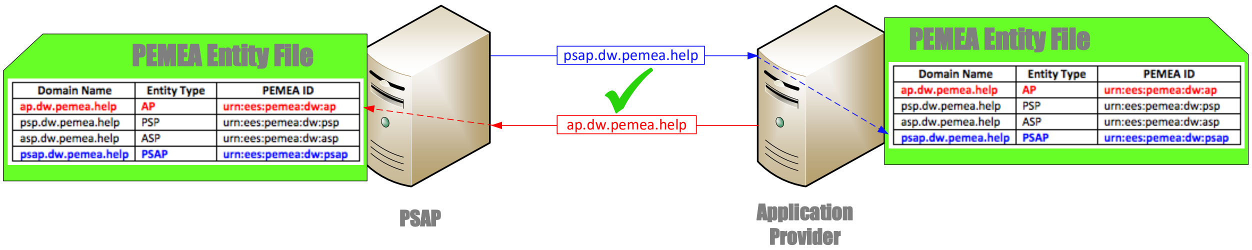
*Table 1: AP valid received messages*

| Message type Received | Message Originating From | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✓ | ✓ | ✗ |
| EDS | ✗ | ✗ | ✗ | ✗ |
| EDR | ✗ | ✓ | ✗ | ✗ |
| onCapSupportPost | ✗ | ✓ | ✗ | ✓ |
| SubscriberInfo Request | ✗ | ✓ | ✗ | ✓ |

*Table 2: AP valid messages sent*

| Message type sent | Message Destination Entity | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✗ | ✗ | ✗ |
| EDS | ✗ | ✓ | ✗ | ✗ |
| EDR | ✗ | ✗ | ✗ | ✗ |
| onCapSupportPost | ✗ | ✗ | ✗ | ✗ |
| SubscriberInfo Request | ✗ | ✗ | ✗ | ✗ |

An AP will receive messages from a terminating-PSP or a terminating-PSAP indicating that the data message was successfully received. When this occurs, the AP locks all further communication for the user session to that terminating-PSP or PSAP. This mean that only the terminating node will have access to any further information about the user and the emergency. It is highly recommended that this initial message from the terminating-PSP or PSAP be an onCapSupportPost message and this is why its inclusion from the AP in the EDS is highly recommended.



| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

*Figure 3: PSAP to AP authentication*

## 3.2 | PSP CONNECTIVITY

**The PSP can interconnect with all PEMEA nodes, but it will not accept connections from all nodes types. Further, a PSP will only accept connections from APs that it considers neighbours (those that it has sponsored), and even then, only those that are in the current PEMEA entity list.**

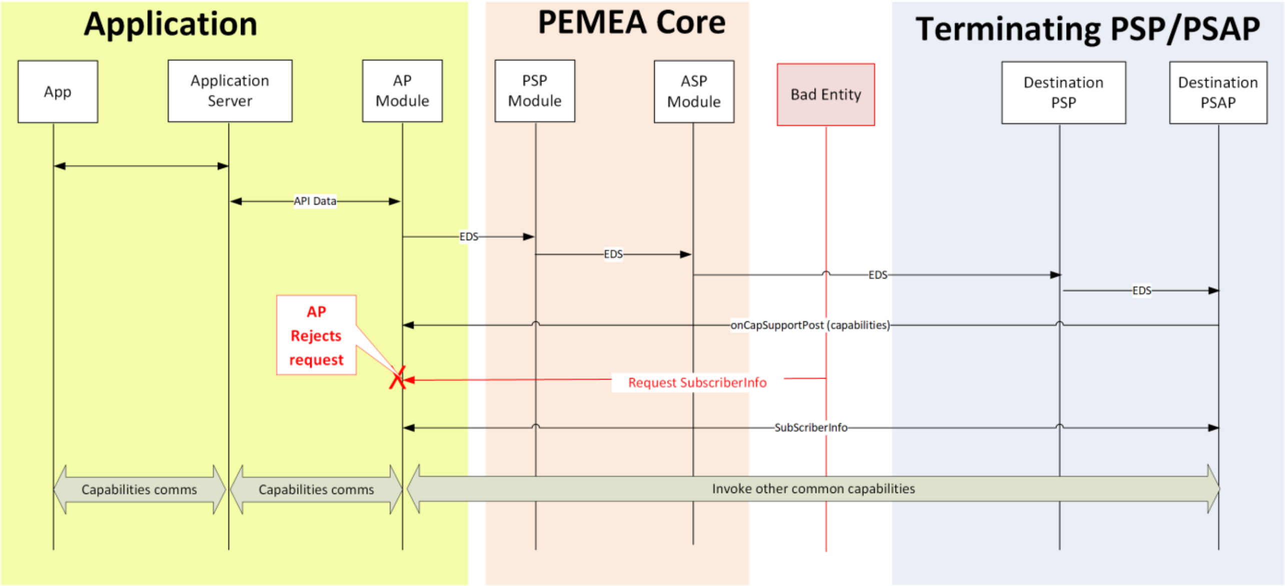


*Figure 4: AP locking data request to terminating node*

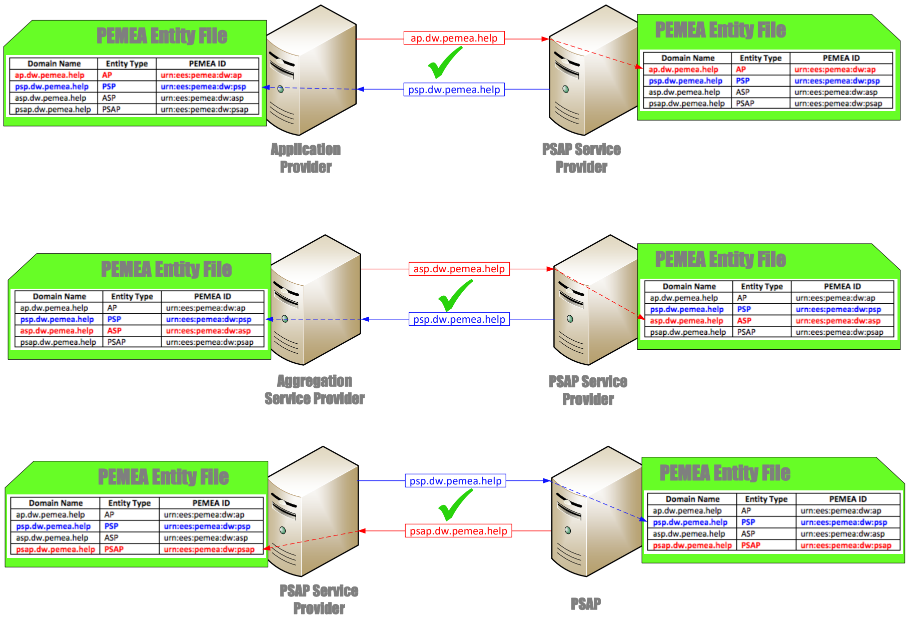
*Table 3: PSP valid received messages*

| Message type Received | Message Originating From | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✓ | ✓ | ✓ |
| EDS | ✓ | ✓ | ✓ | ✗ |
| EDR | ✗ | ✓ | ✓ | ✓ |
| onCapSupportPost | ✗ | ✗ | ✗ | ✗ |

*Table 4: PSP valid messages sent*

| Message type Sent | Message Destination Entity | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✓ | ✓ | ✓ | ✗ |
| EDS | ✗ | ✓ | ✓ | ✓ |
| EDR | ✓ | ✓ | ✓ | ✗ |
| onCapSupportPost* | ✓ | ✗ | ✗ | ✗ |
| SubscriberInfo Request* | ✓ | ✗ | ✗ | ✗ |

* Only valid for a terminating-PSP.



| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

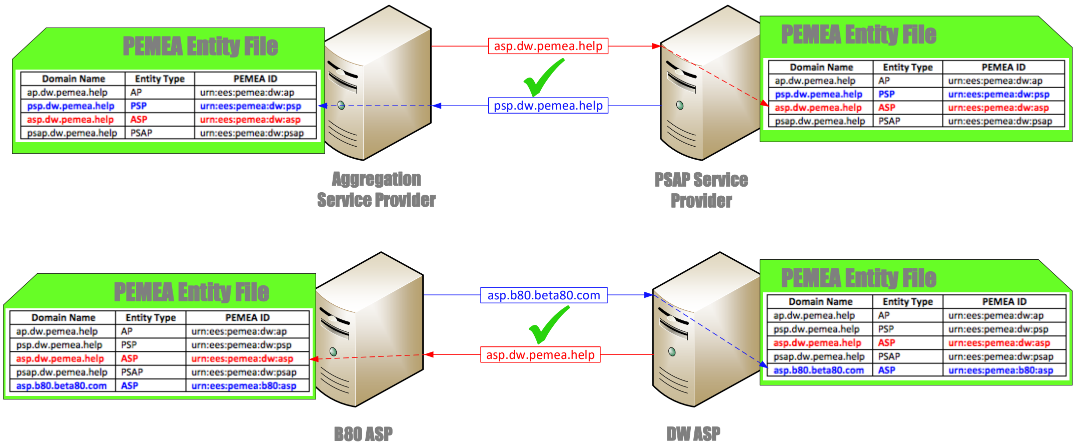
| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

*Figure 5: Allowed PSP entity connections*

## 3.3 | ASP CONNECTIVITY

**The ASP is the top level routing node in the PEMEA network. Consequently, it must only ever accept connections from PSPs or other ASPs. If the ASP encounters an error, then it may send an error message to the AP. The ASP never tries to contact an AP in any other circumstance and never attempts to contact a PSAP**.



| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |
| asp.b80.beta80.com | ASP | urn:ees:pemea:b80:asp |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |
| asp.b80.beta80.com | ASP | urn:ees:pemea:b80:asp |

*Figure 6: ASP connectivity*

*Table 5: ASP valid received messages*

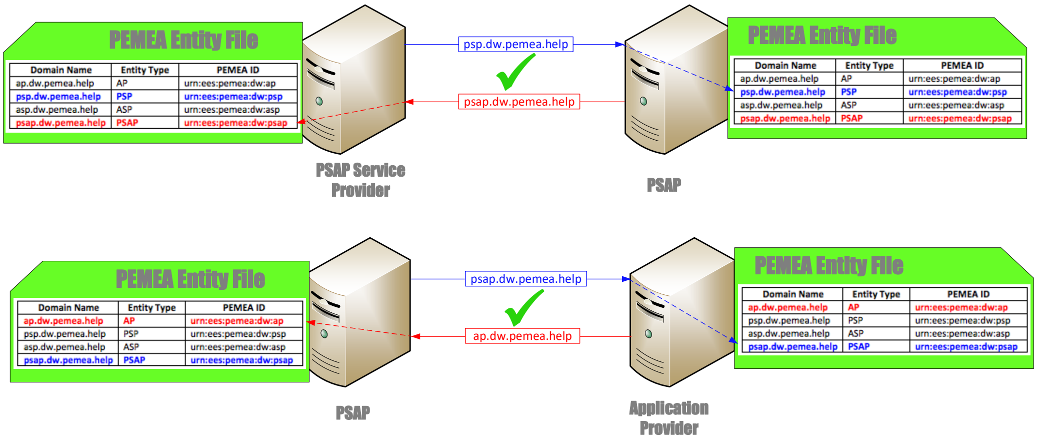
| Message type Received | Message Originating From | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✓ | ✓ | ✗ |
| EDS | ✗ | ✓ | ✓ | ✗ |
| EDR | ✗ | ✓ | ✓ | ✗ |
| onCapSupportPost | ✗ | ✗ | ✗ | ✗ |

*Table 6: ASP valid messages sent*

| Message type Sent | Message Destination Entity | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✓ | ✓ | ✓ | ✗ |
| EDS | ✗ | ✓ | ✓ | ✗ |
| EDR | ✗ | ✓ | ✓ | ✗ |
| onCapSupportPost | ✗ | ✗ | ✗ | ✗ |

## 3.4 | PSAP CONNECTIVITY

**The PEMEA-PSAP is the final node in the PEMEA chain and will only accept EDS messages from neighbour PSPs. If the EDS message contains an onCapSupportPost attribute, the PEMEA-PSAP will notify the AP that it has received the EDS. Further communication for that user session is then between the PEMEA-PSAP and the AP directly.**



| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

| Domain Name | Entity Type | PEMEA ID |
|---|---|---|
| ap.dw.pemea.help | AP | urn:ees:pemea:dw:ap |
| psp.dw.pemea.help | PSP | urn:ees:pemea:dw:psp |
| asp.dw.pemea.help | ASP | urn:ees:pemea:dw:asp |
| psap.dw.pemea.help | PSAP | urn:ees:pemea:dw:psap |

*Figure 7: PSAP connectivity*

*Table 7: PSAP valid received messages*

| Message type Received | Message Originating From | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✗ | ✗ | ✗ |
| EDS | ✗ | ✓ | ✗ | ✗ |
| EDR | ✗ | ✗ | ✗ | ✗ |
| onCapSupportPost | ✗ | ✗ | ✗ | ✗ |

*Table 8: PSAP valid messages*

| Message type Sent | Message Destination Entity | | | |
|---|---|---|---|---|
| | AP | PSP | ASP | PSAP |
| Error | ✗ | ✓ | ✗ | ✗ |
| EDS | ✗ | ✗ | ✗ | ✗ |
| EDR | ✗ | ✓ | ✗ | ✗ |
| onCapSupportPost | ✓ | ✗ | ✗ | ✗ |
| SubscriberInfo Request | ✓ | ✗ | ✗ | ✗ |

# 4 | PERSONAL DATA IN PEMEA

**PEMEA is, first and foremost, an architecture for assisting users and authorised agencies in the time of an emergency. Therefore, information associated with and relating to the emergency needs to be transferred between entities.**

Different countries require different information sent to the PSAP during an emergency communication. PEMEA requires some information at call-time to be provided, so that the initial data packet can be delivered to the correct PSAP, but it tries to keep this to the minimal data set possible. Once the data arrives at the PSAP and is confirmed, additional information may be made available to the PSAP on request.

The initial data packet (emergencyDataSend or EDS) contains the following information:

- Message Sequence ID (unique identifier for a message), msgSeq also referred to as the EDS-id
- Route (where the message started and each hop it does through the network)
- callerIds, also called User-IDs (identifier of the user, often the telephone number)
- Capabilities (extensions that the application supports)
- accessData, also called Network parameters (country code, network code, WiFi network identifier)
- Location information (location where the user is at the time of the emergency)
- User-Info reference (reference that a PSAP can use to get User or Subscriber information if necessary)

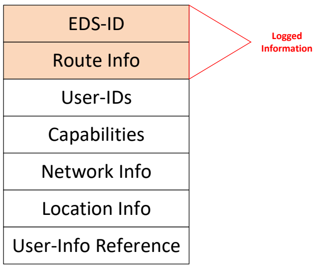


*Figure 8: Basic information in a PEMEA EDS message*

All PEMEA nodes should log the EDS-ID and Route-Info data but no other data. The exception to this is the PSAP that keeps information associated with the call as required by the member state laws. This ensures that only the emergency organisation has access to any private user information. Access to this information is controlled by the PSAP organisation and is subject to their auditing and logging governance.

## 4.1 | PEMEA DATA SETS

When an application initiates an emergency call, it sends data to the AP, often via a third-party Application server. The AP provides APIs for receiving this information and this information comprises the following data groups:

- Personal identfiers
- Location data
- User data

Each of these is explained in more detail below.

### 4.1.1 | PERSONAL IDENTIFIERS

Personal identifiers provide the set of identifiers that can be used to determine “who” is originating the call. For most applications, this is restricted to the calling number of the device: the MSISDN (Mobile Station Integrated Services Digital Network).

The identity being used, the MSISDN, is always passed from the calling entity to the AP at call-time. The MSISDN must never be logged by any PEMEA node except the PSAP. PEMEA forbids the logging or storing to disk of any user identifiers by any node other than the PSAP.

In the PEMEA, it is recommended that Personal identifiers:

- Are only kept in transient memory by the AP for the duration of the emergency session.
- Shall never be logged or stored to disk by:
    - AP
    - PSP
    - ASP
- Shall be sent with all outbound PEMEA EDS messages from ALL PEMEA nodes.
- May be logged at the PSAP.

### 4.1.2 | LOCATION DATA

Location data is always provided with the initial message to the AP when an emergency call is being made. The location data is calculated by the device as quickly as possible, but is still likely to be quite accurate. This initial location data is used by the PEMEA network to determine which PSAP to send the PEMEA EDS message to.

Initial location data:

- Shall be received by the AP and only kept in transient memory for the duration of the emergency session.
- Shall never be logged by the AP.
- May be logged in association with the EDS-ID at the PSP and ASP nodes for route determination auditing purposes in case of error or service failure.
- Shall be sent with all outbound PEMEA EDS message from ALL PEMEA nodes, except for the PSAP.
- May be logged at the PSAP associated by the EDS-ID.

Depending on the capabilities of the application and the configuration of the AP, it is possible for the App to send location updates to the AP. These updates are only ever shared between the AP and the terminating PEMEA entity (PSP or PSAP).

Updated location data:

- Shall be received by the AP and only kept in transient memory for the duration of the emergency session.
- Shall be provided by the AP to a terminating PEMEA node providing that:
    - The node is a validate PEMEA entity;
    - The node is a PSAP or PSP;
    - The node is the same node that registered final receipt of the EDS to the AP (onCapSupportPost);
    - The node requests the location information.
- Shall be requested from the AP, received, stored and logged by the PSAP on request from the call-taker.

### 4.1.3 | USER DATA

The user data capabilities offerred by the PEMEA comply with the IETF SubscriberData from the *Additional Data specification*[3] or the JSON version is defined and referred to as the *UserData specification*[4]. These specifications are similar and quite extensive. They cover the elements below:

- Name
- Age
- Home address
- Languages that user can speak, read/write, sign
- Alternative contact numbers or application handles
- Email addresses
- Next of kin and in case of emergency contacts:
    - Relationship to the user
    - Languages that the kin speak, read/write, sign
    - Ways to contact them:
        - Contact numbers or application handles
        - Email addresses

[3] *https://tools.ietf.org/html/rfc7852*
[4] *https://www.pemea.help/download/nexes-userdata-specification/?wpdmdl=58&*

User data:

- Shall only be received by the AP and only ever stored in transient memory for the duration of the emergency session.
- Shall only be provided by URI in outbound PEMEA EDS messages.
- Shall only be provided by the AP to a terminating PEMEA node when:
  - The node is a validate PEMEA entity;
  - The node is a PSAP or PSP;
  - The node is the same node that registered final receipt of the of the EDS to the AP (onCapSupportPost);
  - The node requests the user data.
- May be logged in the PSAP.

When user data is requested by a terminating node, the AP shall log the identity of the node requesting the data against the EDS-ID and the time that the request was made. The data provided shall NEVER be logged by the AP. This ensures that the AP is able to provide details about who the data was provided to and when.

The PSAP shall log the time that the request for the user data was made by the PSAP call-taker. It shall also log the time that it requested and received the user data from the AP.

## 4.2 | MINIMUM FORWARD DATA SET

**The minimum forward data set in PEMEA is the data required to get the message to the correct PSAP. This information is transferred from the Application, to the AP, through the PSP, the PEMEA network at large, and finally the terminating PSP and PSAP. While all of these nodes are trusted within the PEMEA network, it is important to minimise what data is sent.**

In PEMEA, at call initiation, the Application sends the user-id and the location of the device to the AP, which then forwards this information through the PEMEA network to the terminating PSAP. Where the user-id is the MSISDN of the caller, this solution is no different to the cellular mobile networks where calling number and location are conveyed in the same message to the PSAP at call-time. PEMEA mandates which nodes may store what data and under what circumstances, previous sections of this document prescribe how PEMEA ensures the sececy and integrity and management of this information to ensure adherence to the GDPR edict.

No information other than this basic set is sent through the PEMEA network. All other information is accessible only to the terminating PSP or PSAP and only if the Application has indicated to the AP that it may be provided.

### 4.2.1 | MINIMUM DATA SET LOGGING

Transaction and operations through the PEMEA entities are logged and stored. However, what information is associated with the transaction is dependent on the PEMEA node type.

# 5 | DATA USAGE SUMMARY

This table may be ammended as new features become available in PEMEA.

| Data | AP | | | | PSP | | | | ASP | | | | PSAP | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Stored | Logged | Sent Received | Provided | Stored | Logged | Sent Received | Provided | Stored | Logged | Sent Received | Provided | Stored | Logged | Sent Received | Provided |
| Personal Identifier | M | N | S,R | N/A | M | N | S, R | N | M | N | S, R | N | DB | Y | R | N |
| Location data | M | N | S, R | Y-> | X | Y | S, R | N | X | Y | S, R | N | DB | Y | R | Y<- |
| User data | M | N | R | Y-> | X | X | X | X | X | X | X | X | C | C | N | Y<- |

The above table provides a summary of what private information is used in PEMEA, how it is stored and how it is made available.

- N means action not performed on the data type.
- N/A means that the action is not applicable to the data type at the node.
- DB means that the data may be stored temporarily in a database.
- C means that the data is stored in the manner described based on configuration desired by the managers of the node.
- M means that the data is stored in memory only and is never written to disk.
- S means that the data is sent to another PEMEA node in an EDS message.
- R means that the data is received, either from another PEMEA node in an EDS message or via an API.
- Y means that the data is stored in the manner described.
- Y-> means that data may be provided if requested.
- Y<- means that data may be requested.
- X means that data is not accessible to the node.

# 6 | ABBREVIATIONS, TERMS AND REFERENCES

## 6.1 | ABBREVIATIONS AND TERMS

| | |
|---|---|
| AP | Application Provider |
| **App** | Application |
| **ASP** | Aggregating Service Provider |
| **EDS** | Emergency Data Send |
| **EENA** | European Emergency Number Association |
| **ETSI** | European Telecommunications Standards Institute |
| **GDPR** | General Data Protection Regulation |
| **MS** | Member State |
| **onCapSupportPost** | Message from terminating PSP/PSAP to AP indicating shared capabilities |
| **PEMEA** | Pan-European Mobile Emergency Application |
| **PRA** | PEMEA Registration Authority |
| **Pr** | PEMEA interface between PSP and ASP |
| **Ps** | PEMEA interface between AP and PSP |
| **PSAP** | Public Safety Answering Point |
| **PSP** | PSAP Service Provider |
| **TLS** | Transport Layer Security |
| **TS** | Technical Specification |

## 6.2 | REFERENCES

*Emergency Communications (EMTEL); Pan-European Mobile Emergency Application,* ETSI TS 103 478 V1.2. 1 (2020-03).

*A Presence-based GEOPRIV Location Object Format*, RFC 4119, December 2005.

*Additional Data Related to an Emergency Call*, RFC 7852, July 2016.

*IANA language tags registry.*

*Project NEXES UserData Specification Version 1.0*

## 6.3 | INFORMATIVE REFERENCES

*HTTP Over TLS*, RFC 2818, E. Rescorla, May 2000.

International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes", ISO Standard 3166- 1:1997, 1997.

International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions - Part 2: Country subdivision code", Standard 3166-2:1998, 1998.