DuarteFerreira

By EU person you should mean someone that was in EU soil when the data was gathered. You don't need to be a resident.

mattf

boop beep

elasticguest8626

... or where any part of the processing takes part in the EU

Bin

wow.. that is broad.

james_at_blupoin

From Article 3: “This Regulation applies to the processing of personal data of data subjects who are in the Union “

ⓘ Kyle is now known as Guest48110

james_at_blupoin

From Recital 14: "... whatever the nationality or residence of natural persons..."

wiktor_

appropriate ;-)

well that clears things out!

elasticguest4079

What about if you have a commercial arrangement with an EU company and they call your helpdesk and provide a business email address and business telephone number? From what I understand, if the data is being used to enable a commercial transaction, then CONSENT is not required, it is IMPLIED and the protection mechanisms for that type of data are l

imited?

DuarteFerreira

GDPR only afects individual people not companies

~invidual peaople data

james_at_blupoin

a *business* email and phone number are not personal data

elasticguest8626

Might be an SMB where these are the same

elasticguest4079

That's what I thought as well guys.. Thanks Duarte and James.. appreciate the confirmation.. We are still checking with legal..

bladecruze

hi

HansPrengel

Well ... when a business e-mail contains a name it very well might be personal data.

elasticguest8626

In any case if the data subject leaves the data to support a specific purpose then for that purpose you can store and process it, but not use it for other purposes

elasticguest4818

is the GDPR applying to the UK? will it go through and be kept after the brexit next year?

elasticguest2117

Does a company apply to the GDPR after MAY or does the company just have a strategy to comply to the GDPR?

toshiyuki

Does this refer to just data being collected behind the scenes? Like you may have an app which has a user base where you ask the user for some profile information

elasticguest1520

where is the video link? I can't see video

elasticguest8626

No also openly

elasticguest4079

There is no application to GDPR, there is no certification either..

Guest48110

https://www.elastic.co/webinars/gdpr-compliance-and-elasticsearch

james_at_blupoin

GDPR will be enforced in the UK post Brexit - that's been confirmed by the UK government

elasticguest9834

Video link: https://www.youtube.com/watch?v=QCV1oX6QAvE

elasticguest4079

Not just a strategy, you need to have the required controls in place by May 25th, @elasticguest2117

elasticguest6764

A lot of the data that we store in ElasticSearch has been denormalized. However, in reality there could be a lot of connected data scattered across multiple indices and possibly clusters. Sometimes this is more of a graph.

What features in ElasticSearch are available for us to link these records so that tracing the connections and wiping out those records can be removed in all places if requested by the owner of the records.

SimonL

@elasticguest4079 thanks, was wondering aswell

Loek

GDPR is applying in UK before brexit. There is no clarity yet on the status of GDPR after Brexit AFAIK

Rutger

every visitor of a website sends an IP address. These are usually/always stored in webserver logs. Does that mean that any website stores Personal Data?

PaulBroon

yes

Loek

The GDPR policy is already in effect today, and in May 2018 the enforcement will start. It is not enough to just have a strategy

PaulBroon

unless you delete the last octet

james_at_blupoin

Loek - see http://www.blplaw.com/expert-legal-insights/articles/gdpr-and-brexit-uk-government-unveils-data-prot...

elasticguest4079

I have a list of all the EU personal data REGEX patterns for EU member states, has anyone tried using that approach to FIND where they may have sensitive data?

Loek

thanks james!

ⓘ Loek is now known as Loek_Elastic

linker3000

@Loek - Based on ICO info: • What will happen if/when the UK leaves the EU? Will we still need to be GDPR compliant?
Yes, because the UK has committed to adopting the GDPR as law in this Country, and it will also apply if you want to trade with or within an EU member state.

Loek_Elastic

@elasticguest6764 Elasticsearch treats all data inside of it (petabytes, if you must) as searchable data. Hence it is possible to find all data associated with an email address, customer number, tax number, etc. in seconds. If key identifiers are equal across different indices, we can use X-Pack Graph to visualize this and find the to-be-deleted do
cuments
Thanks linker3000, seems clear that we will see something very similar to GDPR in UK post-Brexit

elasticguest4079

If you kill the last octet of the IP address, you've destroyed forensic trails that are required to provide assessment during a data breach investigation.. How is that even helpful? There is a GDPR article that states you need to notify the relevant data protection authority within 72 hours of a breach. If you've removed the last octet, how can you
run reverse forensics??

elasticguest4185

The reminder email said this webinar would begin at 6 pm/18:00 CET, but when you click the link it says it started 17:00 CET

elasticguest8123

The screen froze

elasticguest9834

Video recording and slides will be emailed to all registrants - you can also go back in time and watch the video from beginning.
https://www.youtube.com/watch?v=QCV1oX6QAvE

Bin

looks like fine to me so far, red box around "data protection and crypto&pseudonymization"

PaulBroon

@elasticguest4079 If you deleted the last octet, you don't have personal data anymore, so no need to notify anyone. Or are you storing other personal data along with IPs?

Loek_Elastic

@elasticguest4185 it seems that the US switched to summer time just this weekend, that might be an explanation

ⓘ elasticguest4818 is now known as Andy73

Guest48110

I think the idea is that you have a data breach, you are using the Elastic stack to store server access and would like to use those access logs to help figure out the extent of the breach etc. @PaulBroon

Loek_Elastic

We're sorry for that @Andy73, we will have a recording of the event for anyone that might miss it

OviBoboc

@elasticguest4079 - you want to rotate logs as often as possible and encrypt the ones at rest, that will minimize the amount of data in case of a breach

Loek_Elastic

Indeed we can use X-Pack Security to provide a Audit log of who accessed what, and when. Also, it can be used to tell data subjects when the organization has recorded their information, which is another GDPR requirement

Andy73

thank you, I don't have problem with the video, working fine

elasticguest4079

You may have a data breach that has nothing to do with personal data, what about payment card data, customer files etc. that you need log files to do forensics on? What about threat intel sharing?

OviBoboc

If it has nothing to do with personal data, GDPR does not apply

elasticguest4079

Yeup, I get that

PaulBroon

In such cases you would probably need to do public announcements, just like companies like Sony did. If you can't identify affected individuals, you need to try to reach as many as possible through means like newspapers.
Alternatively, you could send out mass mails to all customers.

elasticguest4079

I'm finding some portions of GDPR are discursive and defeating on other GDPR articles, I'm waiting for some of this to be shaken out and some case law around it..
Often law enforcement wants full logs to help investigate attribution..

Loek_Elastic

@elasticguest4079 GDPR is unfortunately not very clear on all of those issues. Indeed case law is what the industry is waiting for

Andy73

PCI DSS give rules and standards on payment data

PaulBroon

Financial data are not protected by GDPR by the way. It's not considered personal even though it seems weird (at least to me).

Loek_Elastic

indeed, it would be perverse if I have a right to delete all logs related to my activity on a system, if I am an attacker.

elasticguest4079

Andy, some the PCI DSS v3.2 goes against what is in GDPR, so an eCommerce site that is taking payment card either though direct form fields or tokenizaition/hosted page where you are required to keep full logs under PCI for a specific period of time may go against certain GDPR articles in trying to remove personal data..

tom_callahan

No mention on the requirement for encryption of all data flows?

james_at_blupoin

4079 - in that case, you have a lawful basis to keep that data for that period of time and to refuse to delete data at a data subject's request

PaulBroon

Exactly.

Loek_Elastic

X-Pack Security has end to end TLS out of the box

elasticguest7283

TLS is in the X-Pack

PaulBroon

If national law requires you to store transactional data for 10 years, GDPR won't say anything else.

tom_callahan

What if you want an open source solution instead of X-pack?>

linker3000

@tom_callahan - nope, there's guidance and suggestions in the GDPR, but no specifics like mandating encryption of traffic

tom_callahan

@linker3000 interesting, I was under the idea that it was required based on previous webinars

GS

can the data be anonymized before it is indexed in elastic during the first stage itself, instead if anonymizing during the protect stage?

PaulBroon

Within GDPR you only have to state how long you store the data and for what reason (e.g. national law)

elasticguest4509

financial data not protected not weird at all if you consider the consumer credit legislation that is indeed barbarian in terms of respect of human rights as no consent is required to archive, mangle and disrupt individuals financial data

Loek_Elastic

@tom_callahan we check X-Pack specifically to support GDPR requirement

elasticguest8405

any advice (or best practices) for implementing Pseudonymization and at the same time keep the benefits of elasticsesearch's search and aggregation capabilities?

OviBoboc

GDPR doesn't say you cannot keep the logs, quite the opposite. You are allowed to collect data without consent for the purposes of detecting fraud and preventing unauthorized access and maintaining security of the systems. You just have to protect the data and delete when not needed anymore

elasticguest3696

XPACK not necessary for TLS/SSL

Loek_Elastic

@GS yes, Logstash can anomymize/pseudonomize before ingestion

elasticguest7283

Even IP addresses can be considered as personal data if it can be associated with a natural person

Clovertex

Do you have any reference architectures specific for GDPR

elasticguest4079

Thanks OviBoboc, that's what I thought..

linker3000

Best ot gets: "Article 30 of the GDPR:
1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks

represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
"

elasticguest6000

If we delete data from a user, what do I need if I need to restore a backup?

elasticguest1555

Hi, Mike.

elasticguest3688

when transferring a data record that contains pseudonymized online identifiers and a link to a page where the underlying personal data is viewable, does that record constitute personal data even though the data record itself contains none?

elasticguest1555

Thanks, nice webinar

Loek_Elastic

@8405 yes we do have that, let's talk ,

PaulBroon

@elasticguest7283 IP addresses ARE personal data if stored in full length.

elasticguest1555

a little bit pitty - slides are not sharp, couldn't read

elasticguest6393

how the right to be forgotten migh affect for example audit logs? we need to know the "who" made the change

Loek_Elastic

TLS needs to be enalbed end to end, including between data nodes (in our view), which is what X-Pack does

elasticguest9047

do all companies have to comply or is there some threshold size ?

elasticguest1555

would you provide slides somwhere after?

Loek_Elastic

@Clovertex yes we can apply this to your architecture

elasticguest5309

The UK is writing GDPR into UK law so GDPR will continue after Brexit

PaulBroon

companies below 250 staff members are not required to comply but only if personal data is not processed automatically

Loek_Elastic

thanks @1555!

james_at_blupoin

PaulBroon - that's definitely not true

PaulBroon

there are some exemptions to that though

rich_

Does GDPR apply to government departments? Passports etc

elasticguest4079

IP addresses is a big ovvereach within GDPR, due to the amount of CDNs, redirectors, proxies, anonmyizers, it doesn't ALWAYS apply to the individual that is visiting your website.. In many cases it's an anonymized DHCP pool that a cable/DSL provider issues..

OviBoboc

@rich_ - Yes, and they are required to have a DPO

elasticguest5769

What is the average time to implement a GDPR Project with Elastic?

elasticguest8626

cable/DSL provider can de-anonymize ... they know who got which IP address when

jek

great question

elasticguest8626

this is enought to make it personal

elasticguest4767

If a user specifies a separate Billing Contact (possibly outside the EU), is that contact considered a separate data subject?

elasticguest6426

Question: In cases where the machine data contains IP addresses does GDPR differentiate between public address space or private address space?

elasticguest1555

What do you mean about data subject rights, if they data are proceeded in blogs, websites, i.e. private bloggers - have to follow GDPR requirements, or what?

elasticguest8626

In theory yes

elasticguest4509

where do you post questions for the speaker?

elasticguest1008

What can you tell us about personal data on/of employees in the EU and circumstances under which GDPR applies?

elasticguest7283

how is the pseudomasation working in Logstash, is the token a hash of the original value? which would make it attackable by rainbows tables like approach

james_at_blupoin

1555 if that data relates to EU Citizens or residents - yes, absolutely

Loek_Elastic

please ask questions right here
there is a team sending them to Mike

elasticguest4509

all right

Loek_Elastic

@1008 personal data of employees, if based in the EU or at any time located in the EU, is considered personal data in GDPR

PaulBroon

@elasticguest1008 What do you want to know? Employees have similar rights as customers.

elasticguest1196

Is there any special mechanisms to ingest data using logstash

elasticguest9818

How will it impact social media surveillance

elasticguest4509

QUESTION: how about assure that data remains available for historical, law enforcement and other preservation and documentation purposes?

Loek_Elastic

@7283 you can use a hash indeed. If you seed it by a random seed, rainbow tables will no longer work
@9818 do you mean government surveillance?

elasticguest6000

Hi Mike, If a person want do erasure his information, we need to delete on all backups?

elasticguest1008

@Loek yes, but the employment relationship can limit application of GDPR - i'm asking how that has been defined in understanding of GDPR (so far)

PaulBroon

@elasticguest6000 Theoretically yes

g1_4all

QUESTION: DOES ELASTIC STACK Supports ENCRYPTING AND DECRYPTING THE SUBJECT DATA?

RobinH

so loud

rich_

Does an overwrite of an ElasticSearch document count as a delete? Is it more efficient to overwrite than delete?

Lital

Hi, is there a solution for the right to be forgotten requirement of the GDPR ? Ability to delete a personal data of an individual ?

toshiyuki

pseudonimization doesnt make data compliant correct?

elasticguest1555

How about slides? Would you be so kind to provide them for download?

Loek_Elastic

@rich_ an overwrite of a document leads to a deletion of the old version, yes

elasticguest2720

slides will be sent out with the recording

ekaterina

Hello, we are planning using elastic for logging all activities etc. But we still have our database with sensitive data that are distributed in different tables. Is there any way how elastic can help with this? For both searching for these places and putting it in one separate place

elasticguest1555

Or, either - webinar recording, just to rewatch it again?

Loek_Elastic

@g1_4all it can be done, but it does not a discussion
not=need

elasticguest8405

Is an elasticsearch index WITHOUT its `source` documents (that contain personal info) considered masked/pseudonymized?

Loek_Elastic

@ekaterina: Yes we can definitely help with that

elasticguest1555

2720 - thnx, great

g1_4all

can you take me to any documentation for encryption and decryption

Loek_Elastic

@8405 if you have a non-source data structure like inverse index or doc_values, it still allows you to recover the data. So it would not be masked just because of that. Masking can be achieved using our ETL tooling

g1_4all

@Loek_Elastic can you take me to any documentation for encryption and decryption

RobinH

@Loek_Elastic -- I would be interested how Elasticsearch would encrypt / decrypt subject data

elasticguest6987

gdpr have any policy about backup retention? it is the same as data maximum retention?

elasticguest2605

If the user executes 'Right to be forgotten' - and we delete the EU subject, how do we identify the new data coming in - If it was EU subject with 'Right to be forgotten' or completely new? As we don't have any older reference.

elasticguest1008

@PaulBroon i mean what are the limits on exclusions from GDPR that can be put into employment agreemenst?

Loek_Elastic

@g1_4all if you are technical:
https://www.elastic.co/guide/en/logstash/current/plugins-filters-cipher.html but please engage with us ,
@RobinH same answer ^

elasticguest2720

https://discuss.elastic.co/
discuss forum

Loek_Elastic

thank you

elasticguest8405

thanks @Loek_Elastic. how do we do Pseudonymization and still allow for search over personal info text fields?

specimen_raj

Thank you, it was really helpful

elasticguest1196

Es x pack need to purchase to achieve gdpr am I correct

toshiyuki

if your app holds multiple accounts for a user and that user exercises their right to be forgotten, which accounts will you remove?

elasticguest4509

Very interesting thank you - it looks GDPR is a huge opportunity also to look into policies and standardise practices in the sector

RobinH

@Loek_Elastic -- this link is for Logstash -- what about the capabilities in ES when using the API directly (from client applications)?

PaulBroon

@elasticguest1008 I am not sure what you mean exactly, but in general GDPR applies to employees with putting it into the contract specifically.

elasticguest9186

Uh... It said 6 p.m. CET
9 a.m. PST / 12 p.m. EST / 5 p.m. GMT / 6 p.m. CET

elasticguest4509

can you email text of this chat please

elasticguest1053

is it done ?

elasticguest9186

daylight savings time ;-(

g1_4all

@RobinH
@RobinH
@RobinH @Loek_Elastic upvote

jalaj

Who audits data processor processes when the when the processor is in a country that is not a part of the EU?

elasticguest1008

@PaulBroon well, when you read the GDPR it's just not very clear or defined what can be limited by employment agreements and what cannot. for example, think business email of EU employees

elasticguest9834

Chat will be emailed to all as well

elasticguest1555

Actually, very helpful webinar.

Loek_Elastic

@8405 there are many variations of pseudonimization/anonymization/encryption/etc. In your case, you would need to encrypt data from ingest side and query side and then Elasticsearch will understand it internally

elasticguest1196

Okay thanks

elasticguest4509

thank you

RobinH

Thanks -- great webinar!