ZIMBRA FORUM FRANCE

UIC-P ESPACE CONGRÈS PARIS

20 MARS 2018

THE FUTURE'S SO BRIGHT
#ZFF2018

La réunion annuelle de la communauté et des professionnels Zimbra est prévue le Mardi 20 Mars 2018

À l'IUC-P Espaces Congrès
16 rue Jean Rey - F-75015 Paris

Andrew Shingler
Senior Solution Advisor EMEA, Synacor

EASIER
FASTER
STRONGER
SAFER
SMARTER

ZIMBRA & THE IMPACT OF GDPR

DISCLAIMER

I'm not a lawyer!

I've not read the GDPR Regulations from beginning to end!

The following are suggestions and features that could help achieve compliance!

WHAT IS THE GENERAL DATA PROTECTION REGULATION?

GDPR

What

Privacy law that applies to personal data of EU **residents**

Who

Any information relating to an individual whether they can be identified directly or indirectly

Why

Ensures individuals can control how information about them is used

When

25th May 2018

Privacy

It also ensures those holding the information protects it from disclosure

Global

Applies globally to any organization processing information on EU residents

Penalties

Penalties up to 4% (or €20m whichever is higher) for major breaches

zimbra®
A SYNACOR PRODUCT

SO WHAT SHOULD YOU DO?

DON’T

WHAT IS PERSONAL DATA?

As defined in ”Article 4 GDPR Definitions”:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

WHAT DOES THAT MEAN IN REALITY?

- Personal Email addresses
- Work Email addresses
- Physical addresses
- IP addresses
- Social media IDs
- Date of birth
- Place of birth
- Mobile, business and personal phone numbers
- Login names, Nicknames, Gaming IDs etc.
- And on and on and on….

It is an INEXHAUSTIVE list of what may be considered as personal data. The definition of personal data is deliberately wide. And it is contextual too; It is direct and indirect, identified and identifiable, given the context.

WHAT ZIMBRA FEATURES CAN HELP WITH GDPR COMPLIANCE

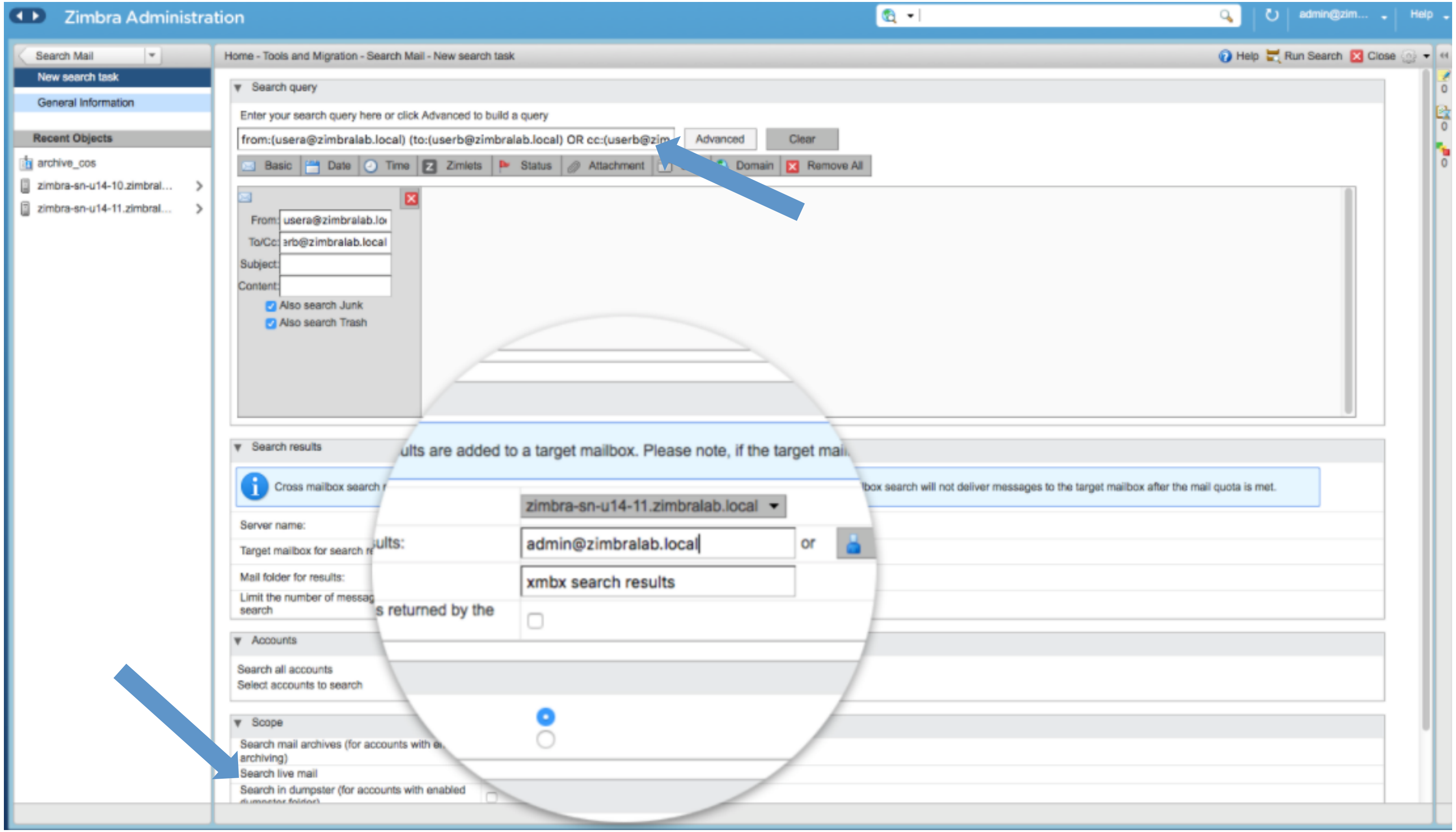
DATA DISCOVERY

- An essential step to meeting the GDPR obligations is discovering and controlling what personal data you hold and where it resides.

- Given the massive volume of data that exists in an unstructured form in a Zimbra platform a technological approach is needed to identify all such data and is an essential step to responding to SARs.

Zimbra Archive & Discovery

ZIMBRA ARCHIVE & DISCOVERY



Enter your search query here or click Advanced to build a query

from:(usera@zimbralab.local) (to:(userb@zimbralab.local) OR cc:(userb@zim

From: usera@zimbralab.lo

To/Cc: erb@zimbralab.local

Subject:

Content:

☑ Also search Junk

☑ Also search Trash

Cross mailbox search results are added to a target mailbox. Please note, if the target mailbox search will not deliver messages to the target mailbox after the mail quota is met.

Server name: zimbra-sn-u14-11.zimbralab.local

Target mailbox for search results: admin@zimbralab.local or

Mail folder for results: xmbx search results

Limit the number of messages returned by the search □

Search all accounts ●

Select accounts to search ○

Search mail archives (for accounts with enabled archiving)

Search live mail

Search in dumpster (for accounts with enabled dumpster folder)

ENCRYPTION

Of the 261 pages of GDPR, the word 'Encryption' appears just 4 times;"

"...implement measures to mitigate those risks, such as encryption.

"...appropriate safeguards, which may include encryption"

"...including inter alia as appropriate: the pseudonymisation and encryption of personal data

"... the existence of appropriate safeguards, which may include encryption or..."

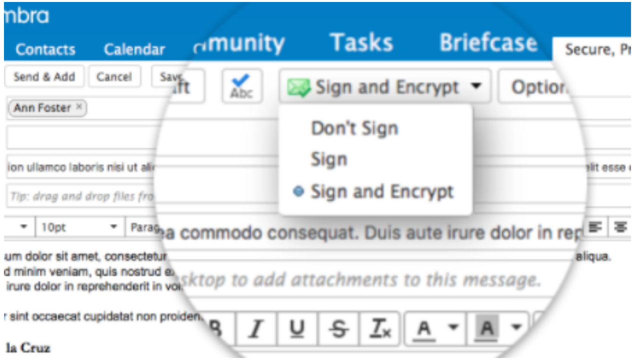
Do the terms 'may', 'such as' and 'as appropriate' indicate that Encryption is mandated by GDPR - I don't believe it does.

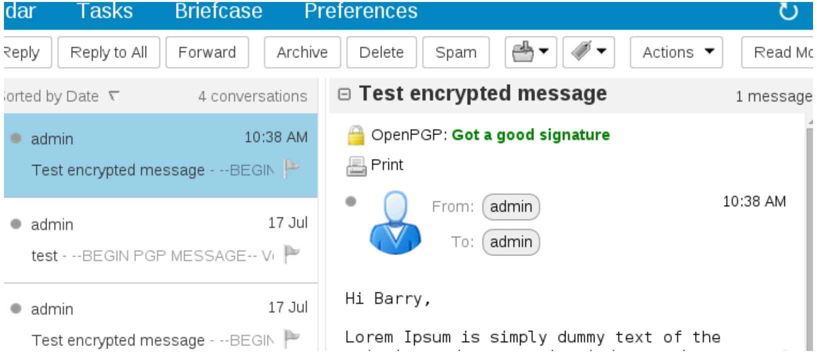
Do these terms suggest that Encryption is an OPTION and a good idea? - Yes, it does.

S/MIME
PGP

ENCRYPTION

- Consider enabling S/MIME encryption
- Open Source PGP options available
- But consider the Pros and Cons
- Encrypt archived backups
- Encryption of end point devices
- What about encryption at rest
- Mobile device encryption





admin Test encrypted message - --BEGIN	10:38 AM
admin test - --BEGIN PGP MESSAGE-- Ve	17 Jul
admin Test encrypted message - --BEGIN	17 Jul

Test encrypted message

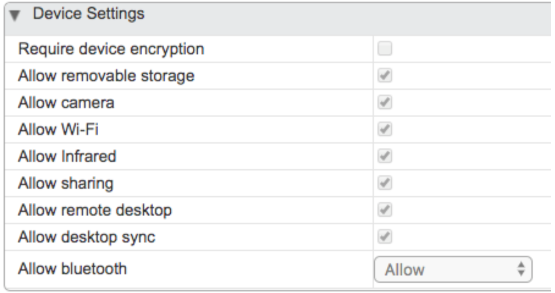
OpenPGP: Got a good signature

From: admin 10:38 AM

To: admin

Hi Barry,

Lorem Ipsum is simply dummy text of the



Device Settings	
Require device encryption	□
Allow removable storage	☑
Allow camera	☑
Allow Wi-Fi	☑
Allow Infrared	☑
Allow sharing	☑
Allow remote desktop	☑
Allow desktop sync	☑
Allow bluetooth	Allow

PERIMETER SECURITY

- Review wiki for best practices
- Enable DKIM and SPF
- Make sure AV signatures are kept up to date
- Should you consider 3rd party solutions?
- Firewall rules
- Tiered architecture – leverage multi-server

DKIM
ClamAV
SPF
Postscreen

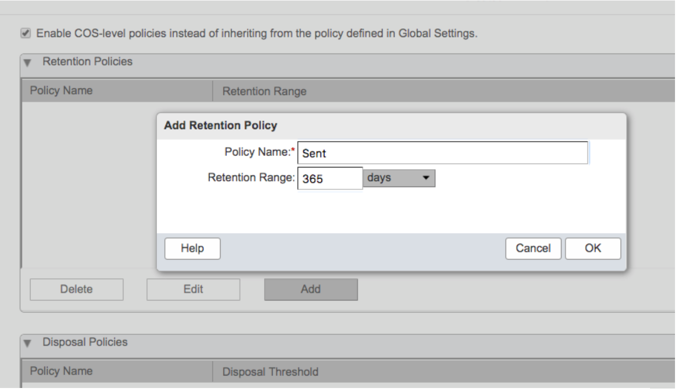
DATA RETENTION

- The emphasis under the GDPR is data minimization both in terms of the volume of data stored on individuals and how long it is retained for.
- GDPR states that personal data shall be kept for no longer than is necessary. (Though regulatory compliance requirements can still prevail)
- Organizations must ensure personal data is securely disposed of when no longer needed.

Retention Policies MDM

DATA RETENTION

- Leverage the retention policies available in Zimbra. The Admin can enforce retention policies at a CoS and per user level
- Don’t forget backups – only keep backup archives needed for DR and compliance
- Zimbra Mobile policies can apply limits to the amount of data synchronized on mobile devices as well as remote wipe and policy enforcement.



☑ Enable COS-level policies instead of inheriting from the policy defined in Global Settings.

▼ Retention Policies

Policy Name	Retention Range

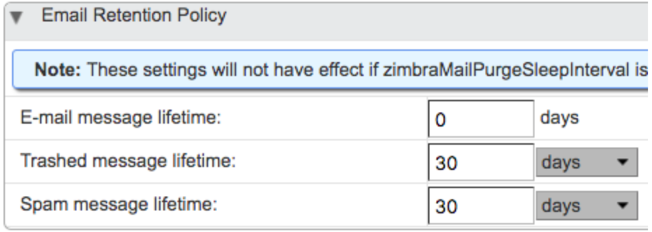
Add Retention Policy

Policy Name:* Sent

Retention Range: 365 days

▼ Disposal Policies

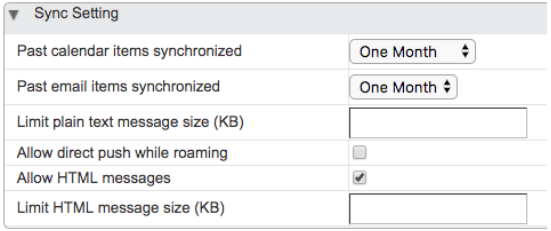
Policy Name	Disposal Threshold



▼ Email Retention Policy

Note: These settings will not have effect if zimbraMailPurgeSleepInterval is

E-mail message lifetime:	0	days
Trashed message lifetime:	30	days
Spam message lifetime:	30	days



▼ Sync Setting

Past calendar items synchronized	One Month
Past email items synchronized	One Month
Limit plain text message size (KB)	
Allow direct push while roaming	□
Allow HTML messages	☑
Limit HTML message size (KB)	

IDENTITY AND ACCESS MANAGEMENT

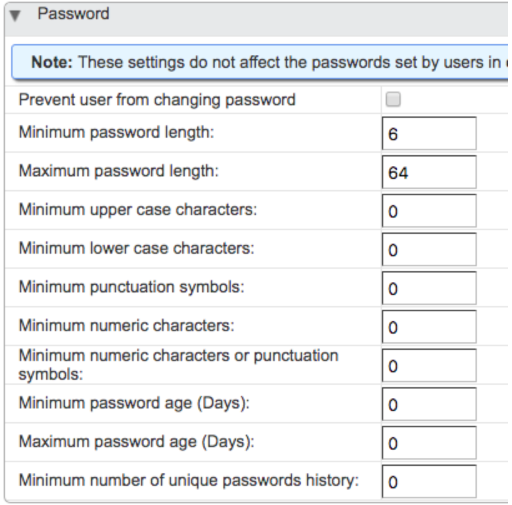
Whether it's critical data or systems, GDPR will require organizations to have the appropriate access policies in place. Your organization should review:

- Administrator privileges
- Ensuring only the right people have access to personal data
- Off-boarding and de-provisioning
- Strengthening authentication

Password Aging & Complexity 2FA

IDENTITY AND ACCESS MANAGEMENT

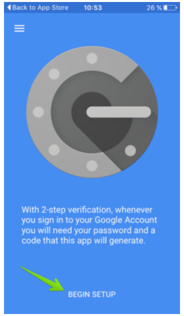
- Setup password policies in CoS
- Enable 2 Factor Authentication
- Fail2ban intrusion prevention
- Monitor audit logs for suspicious activity



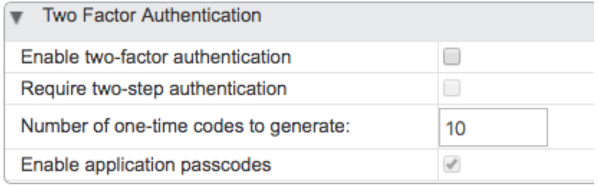
▼ Password

Note: These settings do not affect the passwords set by users in

Prevent user from changing password	□
Minimum password length:	6
Maximum password length:	64
Minimum upper case characters:	0
Minimum lower case characters:	0
Minimum punctuation symbols:	0
Minimum numeric characters:	0
Minimum numeric characters or punctuation symbols:	0
Minimum password age (Days):	0
Maximum password age (Days):	0
Minimum number of unique passwords history:	0



With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.



▼ Two Factor Authentication

Enable two-factor authentication	□
Require two-step authentication	□
Number of one-time codes to generate:	10
Enable application passcodes	☑

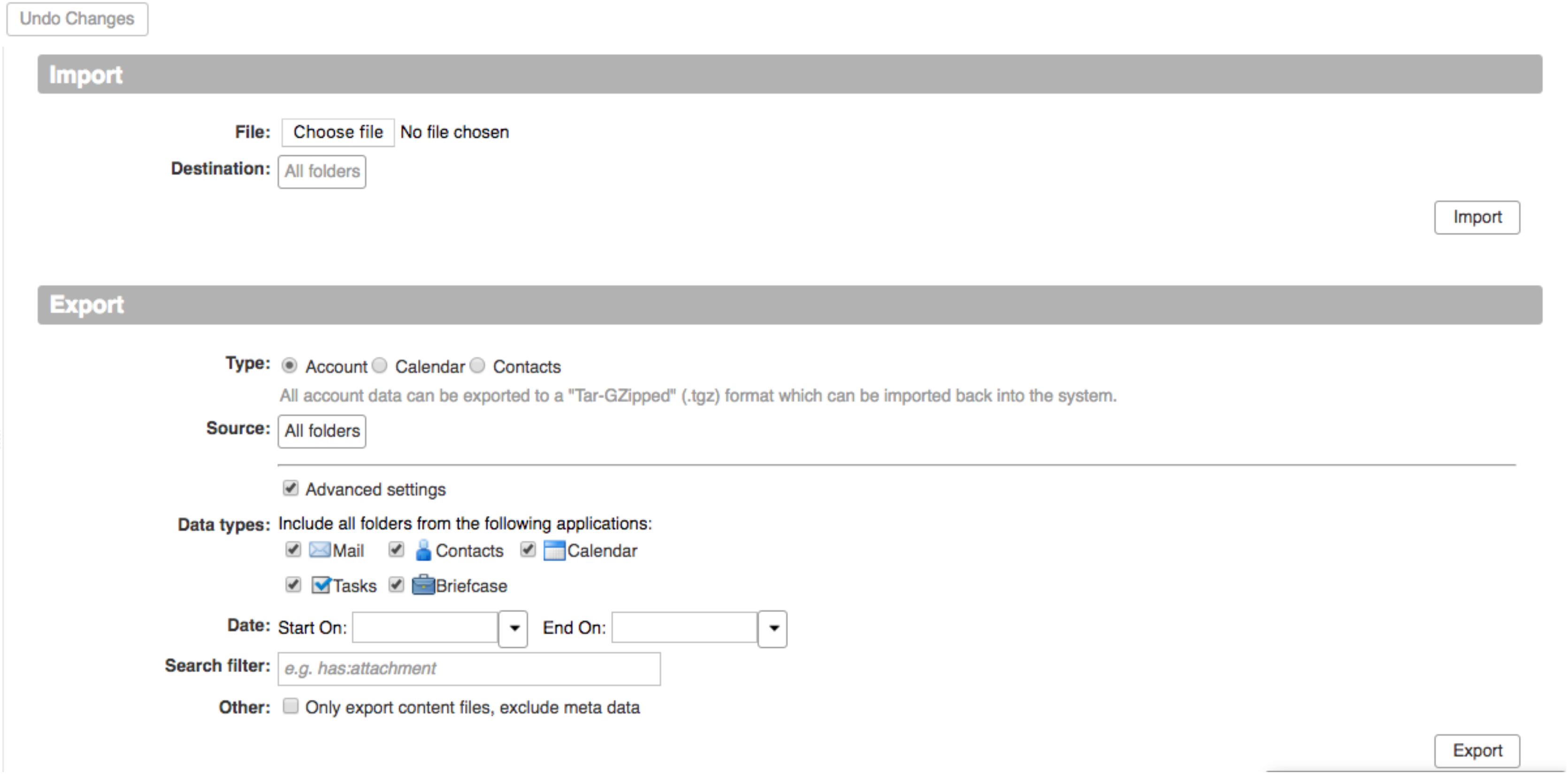
DATA PORTABILITY

Data subjects have the right to request an export of their data in a usable format that can be given to another vendor or service provider to import into its service.

Enabling customers to perform their own export of personal data through a secure, self-service web interface is a good way of balancing access and economics.

Import
Export

DATA PORTABILITY



Undo Changes

Import

File: Choose file No file chosen

Destination: All folders

Import

Export

Type: ● Account ○ Calendar ○ Contacts

All account data can be exported to a "Tar-GZipped" (.tgz) format which can be imported back into the system.

Source: All folders

☑ Advanced settings

Data types: Include all folders from the following applications:

☑ Mail ☑ Contacts ☑ Calendar

☑ Tasks ☑ Briefcase

Date: Start On: ▾ End On: ▾

Search filter: *e.g. has:attachment*

Other: □ Only export content files, exclude meta data

Export

OTHER CONSIDERATIONS

- Right to be forgotten (Compliance?, Backups?)
- Intrusion detection & audit logs
- Certification
- Consent (Legitimate interest or positive consent)
- Data sovereignty
- DLP (MyDLP?)

THANK YOU!