

CLAIMS

1. A computer-implemented method comprising:
accessing, by a server system, one or more digital applications, each of the one or more digital applications configured to be accessed by a plurality of users, and each of the one or more digital applications include the compliance content therein;
removing the compliance content from each of the one or more digital applications;
storing the compliance content removed from each of the one or more digital applications in a central repository while maintaining an association between the compliance content and the one or more digital applications from which the compliance content was removed; and
facilitating integration of one or more widgets into each of the one or more digital applications to access the compliance content stored in the central repository, wherein the one or more widgets integrated into a digital application of the one or more digital applications enables a user of the digital application to access the compliance content from the central repository.
2. The method as claimed in claim 1, further comprising integrating the widget with an Application Programming Interface (API) of the digital application to make an API call to the central repository.
3. The method as claimed in claim 2, further comprising:
establishing the API call to the central repository upon selection of the one or more widgets in the digital application by the user; and
facilitating display of the compliance content in the one or more widgets.
4. The method as claimed in claim 1, wherein the compliance content comprises at least one of: legal content or consent language texts.
5. The method as claimed in claim 1, wherein removing the compliance content comprises extracting content from each of the one or more digital applications and matching the content with a known set of keywords related to compliance content.

6. The method as claimed in claim 1, further comprising extracting the compliance content by a reader and extractor module comprising at least one of: a JavaScript Object Notation (JSON) reader; a website reader; an excel sheet onboarding reader; or a Content Repository for Java technology (JCR) extraction module.

7. The method as claimed in claim 1, wherein storing the compliance content for the digital application comprises configuring one or more tags using one or more identifiers of the compliance content, the one or more identifiers indicating at least a type of service or business associated with the digital application.

8. The method as claimed in claim 7, wherein the one or more identifiers of the compliance content comprises at least a service code, a user category code and a locale code indicating a geographical location associated with the digital application.

9. The method as claimed in claim 1, wherein storing the compliance content for the digital application further comprises:

creating a directory of pages in a hierarchical manner, the directory of pages associated with one or more tags related to the compliance content of the digital application;
incorporating the compliance content removed from the digital application into the directory of pages based on the one or more tags related to the compliance content;
and
storing the directory of pages incorporated with the compliance content in the central repository.

10. The method as claimed in claim 1, wherein the compliance content comprises General Data Protection Regulation (GDPR) compliance content.

11. The method of claim 1, wherein each of the one or more digital applications includes a plurality of pages, and further comprising:

parsing the plurality of pages of the one or more digital applications to identify the compliance content prior to removal from the one or more digital applications.

12. A server system comprising:

a memory device comprising stored instructions; and

a processor coupled to the memory device, the processor configured to execute the stored instructions to cause the server system to:

access one or more digital applications, each of the one or more digital applications configured to be accessed by a plurality of users, and each of the one or more digital applications including compliance content therein;

remove the compliance content from each of the one or more digital applications;

store the compliance content removed from each of the one or more digital applications in a central repository while maintaining an association between the compliance content and the one or more digital applications from which the compliance content was removed; and

facilitate integration of one or more widgets into each of the one or more digital applications to access the compliance content stored in the central repository, wherein the one or more widgets integrated into a digital application of the one or more digital applications enables a user of the digital application to access the compliance content from the central repository.

13. The server system as claimed in claim 12, wherein the server system is caused to integrate the widget with an Application Programming Interface (API) of the digital application to make an API call to the central repository.

14. The server system as claimed in claim 13, wherein the processor is configured to execute the stored instructions to further cause the server system to:

establish the API call to the central repository upon selection of the one or more widgets in the digital application by the user; and

facilitate display of the compliance content in the one or more widgets.

15. The server system as claimed in claim 12, wherein the compliance content comprises at least one of: legal content or consent language texts.

16. The server system as claimed in claim 12, wherein the server system is further caused, in connection with storing the compliance content removed from the digital application, to:

create a directory of pages in a hierarchical manner, the directory of pages associated with one or more tags related to the compliance content of the digital application; incorporate the compliance content removed from the digital application into the directory of pages based on the one or more tags related to the compliance content; and store the directory of pages incorporated with the compliance content in the central repository.

17. A non-transitory computer-readable storage medium storing computer-readable instructions that, when executed by a server, causes the server to:

access one or more digital applications, each of the one or more digital applications configured to be accessed by a plurality of users, and each of the one or more digital applications including compliance content therein; remove the compliance content from each of the one or more digital applications; and facilitate storage of the compliance content removed from each of the one or more digital applications in a central repository while maintaining an association between the compliance content and the one or more digital applications from which the compliance content was removed; and facilitate integration of one or more widgets into each of the one or more digital applications to access the compliance content stored in the central repository; wherein the one or more widgets integrated into a digital application of the one or more digital applications enables a user of the digital application to access the compliance content from the central repository.

18. The non-transitory computer-readable storage medium of claim 17, further storing computer-readable instructions that, when executed by the server, causes the server to integrate the widget by establishing an Application Programming Interface (API) of the digital application to make an API call to the central repository.

19. The non-transitory computer-readable storage medium of claim 17, further storing computer-readable instructions that, when executed by the server, causes the server to:

- configure one or more tags using one or more identifiers of the compliance content, the one or more identifiers indicating at least a type of service or business associated with the digital application;
- create a directory of pages in a hierarchical manner, the directory of pages associated with one or more tags related to the compliance content of the digital application;
- and
- incorporate the compliance content removed from the digital application into the directory of pages based on the one or more tags related to the compliance content, wherein the compliance content incorporated into the directory of pages is stored into the central directory.

20. The non-transitory computer-readable storage medium of claim 17, wherein the determination and removal of the compliance content is performed by at least one of: a JavaScript Object Notation (JSON) reader; a website reader; an excel sheet onboarding reader; or a Content Repository for Java technology (JCR) extraction module.