Ante la extensión de los sistemas de tratamiento de datos personales del personal de los ayuntamientos.

Tras la consulta realizada por las secciones sindicales de CCOO en ayuntamientos de la Comarca de l'Horta, debemos hacer algunas precisiones.

Como no podía ser de otra manera en la mayoría de los casos hay empresas privadas detrás de estas iniciativas. Normalmente trabajos típicos realizados por empresas que no conoce la Administración.

Resulta indignante, ver como en lugar de ir ganando en el terreno de la "democracia laboral" generando complicidades y acuerdos con la Representación Legal de los Trabajadores y Trabajadoras (empleados públicos) nos vemos con esa desafortunada y extendida costumbre de considerar a "priori" la culpabilidad del conjunto del personal evidenciando con ello la desconfianza de entrada con la que nos tratan.

CCOO debe solicitar siempre al ayuntamiento, tratar estas materias en Mesa General de Negociación y exigir información sobre el cumplimiento de los requisitos informáticos, puesto que el tipo de datos que pueden querer almacenar pueden ser de nivel alto.

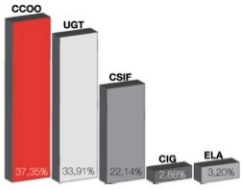
Esto, junto al control de asistencia con huella dactilar o imagen facial (mediciones biométricas) es la ley del embudo. Es decir, quieren tener todos los derechos sobre los trabajadores y trabajadoras pero sin, supuestamente, cumplir con sus obligaciones.

Ahora, más que antes, es imprescindible que las secciones sindicales de CCOO conozcan de forma general los derechos y obligaciones de los empleados públicos sobre sus datos de carácter personal y las consecuencias del mal uso de los mismos tanto por la Administración como por los empleados con las herramientas informáticas de su trabajo.

Todo está interrelacionado, es cierto que hoy en día el abuso que se pueda producir en algún caso es fácilmente rastreable, perseguible y denunciable. Usar los ordenadores o teléfonos del trabajo para disfrute personal deja trazas que conforman pruebas de acciones ilícitas.

En general, las administraciones no suelen abusar de los datos de carácter personal de sus empleados porque es un trabajo delicado y deberá justificar dichas acciones.

Por eso es importante la convocatoria de la MGN y dejar constancia con los responsables del ayuntamiento de que se cumple estrictamente la LOPD para el tipo de datos personales que quieren guardar.



En algún caso, se han pasado al querer almacenar datos sobre Salud.

Algunas de las cosas que hemos podido leer:

Sobre revisión y control por parte del ayuntamiento.

I. El Ayuntamiento se reserva la facultad de revisar periódicamente, el contenido de los distintos buzones de correo electrónico profesional, y así como la facultad de eliminación de todos aquellos mensajes que, una vez analizado su remitente, destinatario, título y fecha por parte del Departamento de Sistemas, se evidencien como ajenos a la actividad del Ayuntamiento.

II. Las mencionadas revisiones se efectuarán por parte del Departamento correspondiente, en el centro de trabajo y dentro del horario laboral.

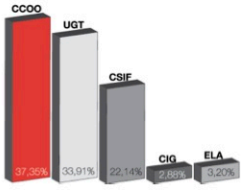
III. Ante la ausencia del trabajador, con motivo de una baja por accidente o enfermedad, día/s libre/s, vacaciones u otra circunstancia semejante, el Ayuntamiento podrá acceder al contenido de la cuenta de correo electrónico del ausente o, en su caso, redireccionar la entrada de mensajes suya a otra cuenta de correo electrónico corporativo, con el único objeto de poder gestionar los asuntos de índole laboral y de interés para la entidad.

En todo caso, siendo considerada la cuenta de correo electrónico corporativo una herramienta de trabajo o de producción laboral, el Ayuntamiento se reserva el derecho a acceder a cualquier correo electrónico que mantenga el profesional tras su cese, temporal o definitivo, en la misma, sin necesidad de solicitar autorización previa, por cualquier causa.

En el ámbito funcionarial podemos considerar que el acceso al correo para vigilancia entra en contradicción con el deber de sigilo o, en su caso, secreto, que puede tener el personal funcionario atribuible a sus funciones.

Por ejemplo, el médico que se encarga de la salud laboral está de vacaciones y no ha sido suplido, entonces, según se pretende, el departamento correspondiente entraría en su correo para “ver” a donde se deber redireccionar los correos pudiendo, por tanto, verse comprometidos datos sensibles sobre la salud de los trabajadores. Asimismo, pongamos que un funcionario o funcionaria está realizando la instrucción de un expediente sancionador de un empleado o empleada y envía información por email al órgano competente. ¿no sería un acceso indebido que personal no competente en la materia accediese al correo sin justificación alguna?

Tampoco queda nada claro realizar revisiones periódicas del email del trabajo. Lo que la jurisprudencia deja claro es que ese acceso se realice ante sospechas de mal uso del correo corporativo, por lo tanto, debe estar plenamente justificado.



En esta materia concreta deberíamos exigir en Mesa Gral de Negociación que en este caso se solicitara un informe consulta a la APD.

Deberemos estar pendientes también como Sección Sindical al posible mal uso de los datos personales que puedan llevar a obtener perfiles.

Ojo. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

En relación a los datos referidos a servicio médico y vigilancia de la salud

Artículo 9 Categorías especiales de datos

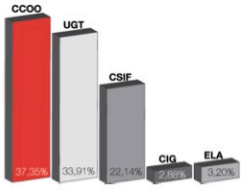
2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Por lo que debemos considerar que dichos datos deberán ser eliminados de forma inmediata una vez el personal sea dado de baja del ayuntamiento.

Por último a tener en cuenta. Sobre la seguridad de los sistemas de tratamiento

En relación con las medidas de seguridad en el ámbito del sector público, en la Disposición adicional primera de la Ley Orgánica 3/2018, se señala que los responsables enumerados en el artículo 77.1 de la citada ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

Guías para las administraciones locales
Agencia Protección de Datos (APD) emite la siguiente guía para administraciones locales:



https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf

la cual, a su vez, hace referencia a las siguientes guías sobre seguridad:
https://www.ccn-cert.cni.es/pdf/documentos-publicos/ens/2449-femp-ens-tomo-1-guia-estrategica-en-seguridad-para-entidades-locales/file.html

Para entidades locales de menos de 2.000 hab.
https://www.ccn-cert.cni.es/pdf/documentos-publicos/ens/2452-femp-ens-tomo-2-guia-para-entidades-locales-de-menos-de-2000-habitantes/file.html

CONCLUSIÓN

La Ley y el Reglamento de Protección de datos OBLIGA a que el personal sea informado de lo que se va a realizar con sus datos de carácter personal.

Desgraciadamente, en algún caso ha habido excesos por parte de trabajadores lo que ha dado lugar a que la ley se haga más laxa para los empresarios y más dura para los trabajadores.

Cuando se pretenda instalar un sistema de tratamiento de datos personales en el ayuntamiento, recomendamos la preparación de una hoja informativa para repartir a los trabajadores y trabajadoras preocupados por la exigencia de la firma de los documentos sobre confidencialidad que les pasarán y que debería contener lo siguiente:

Derechos sobre sus datos personales: Acceso, Rectificación, Supresión, Limitación del tratamiento, Portabilidad y Oposición.

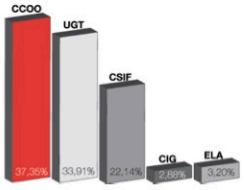
Normativas: Ley Orgánica de Protección de datos y su Reglamento.

Enlaces Web: Guías de protección de datos en las Administraciones locales y Agencia de Protección de Datos.

NO debemos negarnos a la firma de estos documentos, pero SI actuar con el sentido común e ir resolviendo las quejas de los trabajadores de forma puntual.

La legislación actual es:

>>Ley Orgánica 3/2018 de 5 de diciembre de Protección de datos personales y garantía de los derechos digitales.



>> Reglamento (UE) 2016/679 Del Parlamento Europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE

Desgraciadamente el nuevo reglamento ha relajado los mecanismos de protección dejando estos a discreción de la empresa. Por ello consideramos que ha empeorado la seguridad de los datos.